EventTracker
Secure. Comply. Succeed.

EventTracker Enterprise v7.5

Install Guide

Publication Date: June 13, 2014

EventTracker
8815 Centre Park Drive
Columbia MD 21045
www.eventtracker.com

Abstract

This guide will help the users to install and configure EventTracker Enterprise, and verify the expected functionality of all its components.

EventTracker is a reliable, policy driven solution to monitor and manage critical events generated by Windows XP/Vista/7/8/2003/2008/2008 R2/2012/2012 R2 (v7.5 Build 29 and above), Solaris BSM, Unix (SYSLOG), SYSLOG-NG and SNMP devices. EventTracker is an enterprise grade solution that provides real-time alerts, secure warehousing, and flexible reporting.

Target Audience

EventTracker users or system administrators, who wish to install the EventTracker Enterprise Manager.

The information contained in this document represents the current view of Prism Microsystems, Inc. on the issues discussed as of the date of publication. Because Prism Microsystems, Inc. must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Prism Microsystems, Inc. and Prism Microsystems, Inc. cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Prism Microsystems, Inc. MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this Guide may be freely distributed without permission from Prism, as long as its content is unaltered, nothing is added to the content and credit to Prism is provided.

Prism Microsystems, Inc. may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Prism Microsystems, Inc. the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.
© 2014 Prism Microsystems, Inc. All rights reserved.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

Introduction 4
Known Issues for v7.5.53 5
System Requirements 16
Hardware Requirements [Min. Configuration] 16
Software Requirements 16
Pre-install instructions for Local Account and Active Directory authentication v7.5.29 and below versions 18
Create Local User and Group Accounts 18
Create EventTracker User Group 20
Create User 23
Add User to EventTracker Group 25
Create Active Directory User and Group Accounts 30
Create EventTracker Group 31
Create User 34
Add User to EventTracker Group 37
Add User to Local Administrators group 41
Add cross-domain users 42
Add cross-forest users 43
Install EventTracker Manager 44
Pre-install Checklist for EventTracker Manager 44
IIS Settings 45
Procedure to install EventTracker Manager v7.5.53 - Custom 47
Procedure to install EventTracker Manager v7.5.53 - Standard / Collection Point 94
Procedure to install EventTracker Manager for v7.5.29 and below versions 109
User Permission on SQL Server 131
Deploy EventTracker Windows Agent 141
Pre-install Instructions for Windows Agent 141
Pre-install Checklist for Windows Agent 141
Different methods to install EventTracker Agents 142
Deploy EventTracker Windows Agent via System Manager 142

Configure EventTracker Windows Agent 152
Deploy EventTracker Windows Agent – Vista and Above 155
Prerequisites for Windows Agent – Vista and Above 155
Install / Uninstall Vista and above Agent 155
Agent Deployment 155
Secure EventTracker 155
Uninstall EventTracker Windows Agent 156
Uninstall EventTracker Windows Agent via Control Panel 156
Uninstall EventTracker Windows Agent via System Manager 157
Uninstall EventTracker 159

Introduction

EventTracker Enterprise provides a unique combination of capabilities, including:

- Enterprise-wide, Distributed Console Event Management
- Rapid Integration with Active Directory
- USB Device Monitoring
- Automatic Remediation
- Reporting
- Analytics
- Real-time Alerting
- File Integrity Monitoring
- Virtual Infrastructure Monitoring
- Status Tracker

This is the good time to familiarize you with the various product features as described on the Web site (http://www.eventtracker.com/eventtracker/enterprise/) in the brochure of this package. This installation guide is designed as an easy reference, since we recognize the imperative importance of error free and painless installation experience.

***IMPORTANT**: Prism strongly recommends users to refer

'How To Install and Customize Web Server (IIS)' document prior to installing EventTracker 7.5.

Known Issues for v7.5.53

The mentioned below issues are related to v7.5.53 Pre-Installer only.

Q1. I get the error "Failed to map the path '/app_GlobalResources/'." in the browser interface. The workaround for this issue is to re-install IIS Express manually and later run the EventTracker Configuration once again. This error occurs if user has already installed IIS Express RC. Kindly follow the steps mentioned below.

a. Uninstall IIS Express.

b. Download IIS Express 8.0 from

64 Bit:

http://download.microsoft.com/download/1/6/3/163BBBDE-5523-416D-A293-EA0492020E4A/iisexpress_8_0_RTM_x64_en-US.msi

32 bit:

http://download.microsoft.com/download/1/6/3/163BBBDE-5523-416D-A293-EA0492020E4A/iisexpress_8_0_RTM_x86_en-US.msi

c. Install IIS Express 8.0.

d. To run EventTracker Configuration, click **Start**, click **Programs**, and then click **Prism Microsystems**.

e. Select **EventTracker**, and then select **EventTracker Configuration**.

f. Enter valid **User Credentials**, and then select the **OK** button.

Q2. If there are two versions of SQL Express is installed, then what should I do?

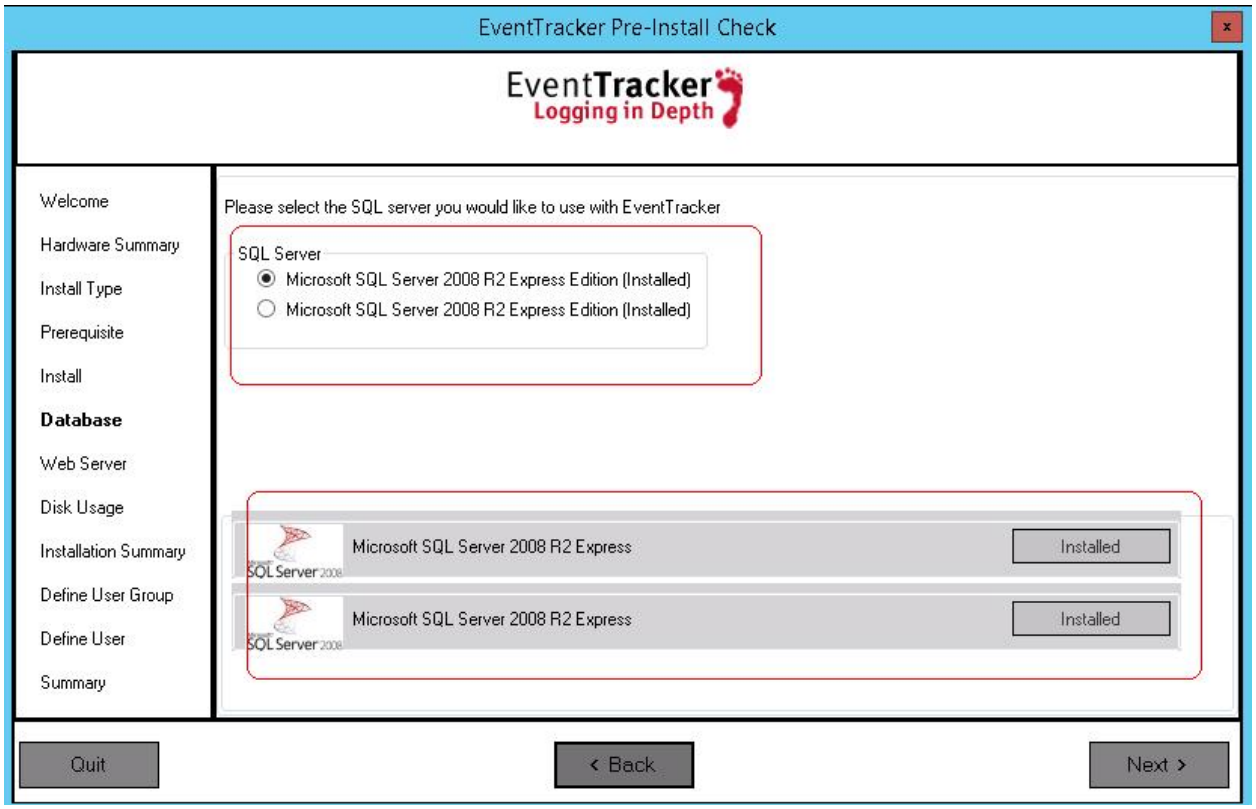


Figure 1

Select either one of those SQL Express installed and proceed further.

Q3. What should I do if IIS Express is not working in Win 2003 (64 bit)/2003 R2 machines?

IIS Express is not supported on Win 2003 (64 bit)/2003 R2 operating systems. Kindly install IIS for the above mentioned OS.

- The installation/setup type will always be **Custom**, and the link to the guide will re-direct the user for detail instruction on how to configure IIS.

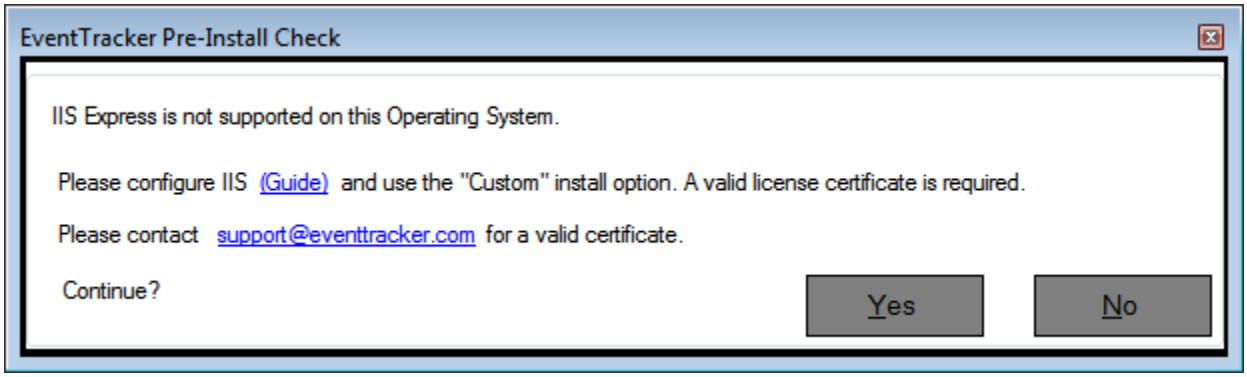

EventTracker Pre-Install Check
IIS Express is not supported on this Operating System.
Please configure IIS (Guide) and use the "Custom" install option. A valid license certificate is required.
Please contact support@eventtracker.com for a valid certificate.
Continue?
Yes
No

Figure 2

- Clicking on **No**, will exit the installation.
- Clicking on **Yes**, will allow user to proceed only with Custom option.
- Users need to get a valid certificate for this type of installation.
- User has to select IIS Web Server only.

Q4. If user X has installed EventTracker and user Y proceeds to install EventTracker on the same machine, then below message is encountered, what should I do?

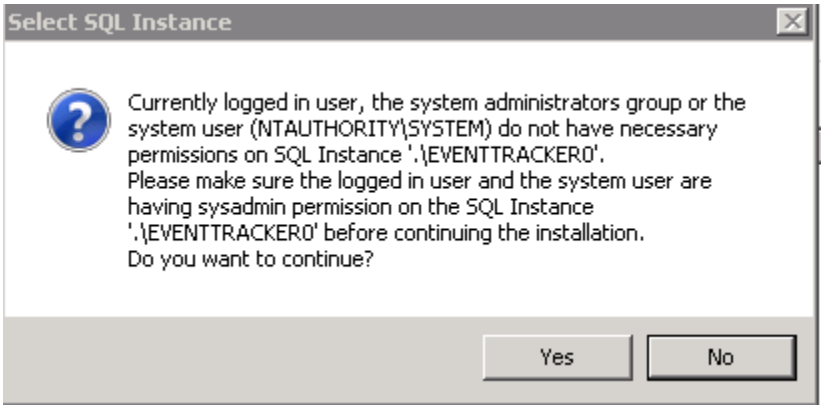

Select SQL Instance
Currently logged in user, the system administrators group or the system user (NTAUTHORITY\SYSTEM) do not have necessary permissions on SQL Instance '.\EVENTTRACKER0'.
Please make sure the logged in user and the system user are having sysadmin permission on the SQL Instance '.\EVENTTRACKER0' before continuing the installation.
Do you want to continue?
Yes
No

Figure 3

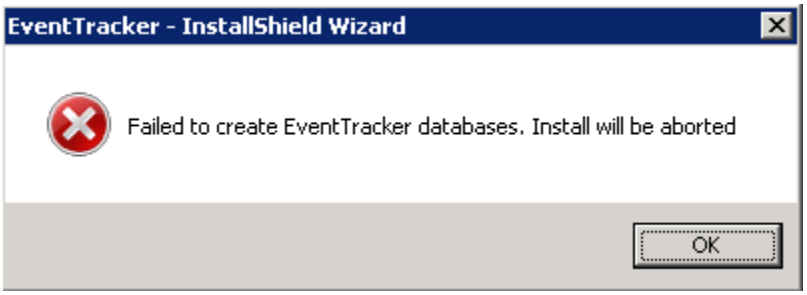


Figure 4

Please make sure that the user who has started the installation is an administrator, and the same user completes the installation. If two users switch between installing the application this issue arises.

The currently logged in user, the System Administrators group, or the System User does not have permissions on respective SQL Instance. Please make sure that the logged in user and the system user are having sysadmin privileges on the SQL instance. For detail instructions to grant sysadmin privilege, please refer User Permission on MS SQL Server.

Q5. What should I do if I get the following error message "PkgMgr.exe has been deprecated."

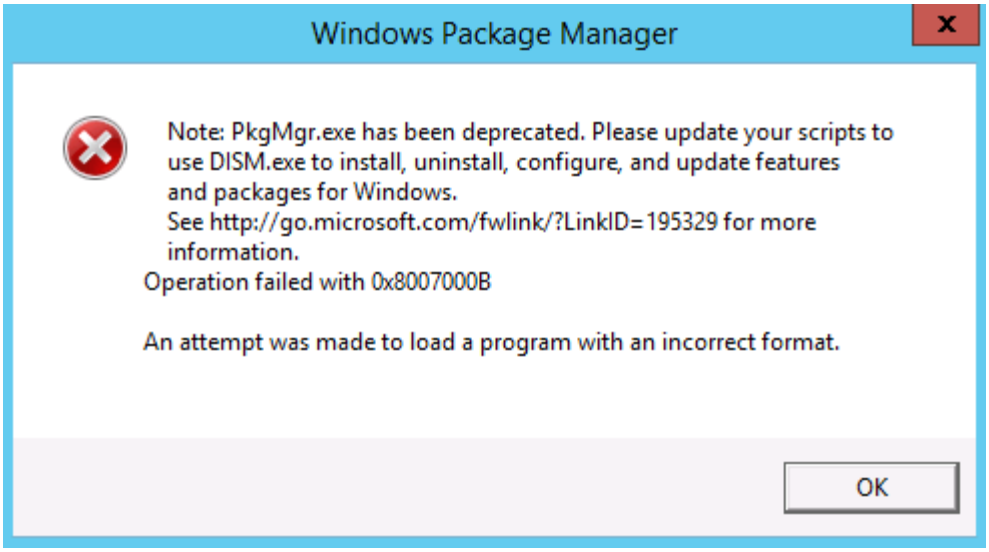

Windows Package Manager
Note: PkgMgr.exe has been deprecated. Please update your scripts to use DISM.exe to install, uninstall, configure, and update features and packages for Windows.
See http://go.microsoft.com/fwlink/?LinkID=195329 for more information.
Operation failed with 0x8007000B
An attempt was made to load a program with an incorrect format.
OK

Figure 5

If you are using **IIS Express** click **OK** and proceed with the installation.

This error message appears if ASP.NET is not installed with IIS. If IIS is already installed, the DISM will enable ASP.NET.

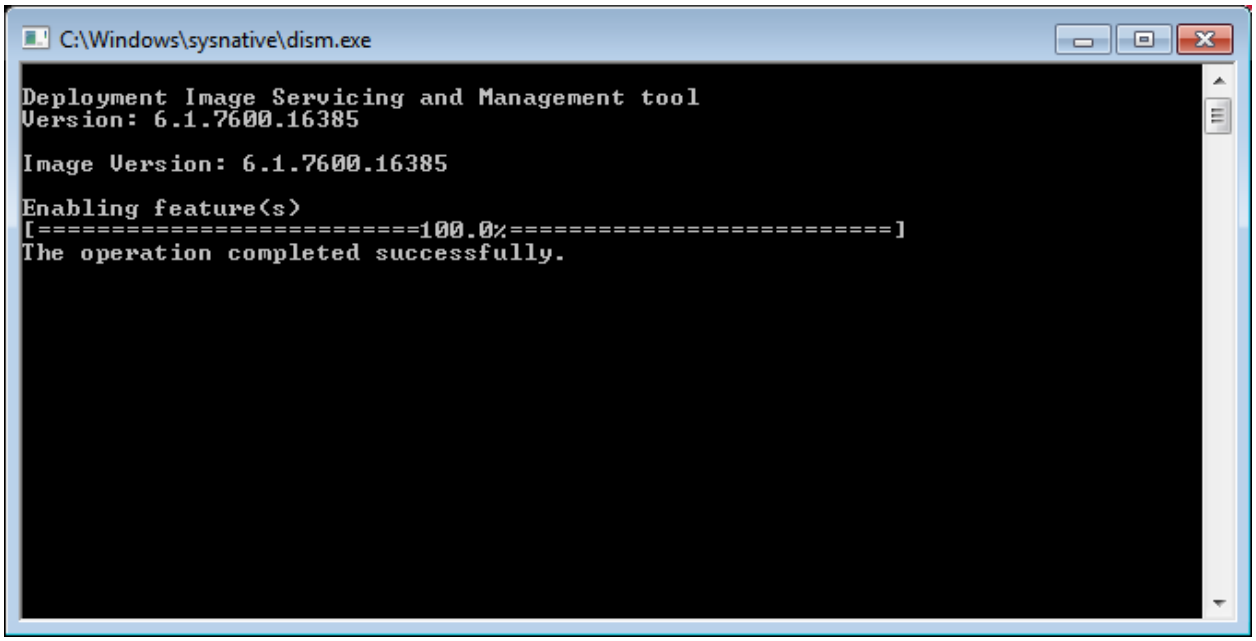


Figure 6

Please make sure that if IIS is installed, then ASP.NET is also installed in the machine. For detail instructions, please refer How To Install and Customize Web Server (IIS).

Q6. What should I do if the pre installer prompts to install IIS Express, even though it is installed?

(OR)

If SQL express is installed via pre-install check, then if you click 'Back', the installer shows SQL express is not installed.

(OR)

What should I do if the message "A reboot is still pending" occurs?

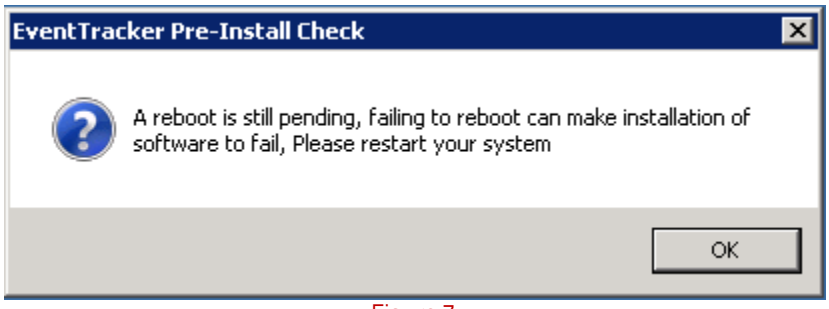

EventTracker Pre-Install Check
A reboot is still pending, failing to reboot can make installation of software to fail, Please restart your system
OK

Figure 7

Sometimes installer does not exit properly. This could be because of the pending reboot for Windows installer/.NET Framework/IIS. Quit the Pre-Installer, restart the machine and run the Pre-Installer once again.

Q7. What should I do, if some components do not work for UK region settings?

Please make sure that the Region settings have been applied to the MS SQL engine, (For Ex: UK region settings). Since EventTracker Setup does not install Microsoft SQL Management Studio, kindly download and install the same.

To configure UK Region settings in MS SQL, please refer UK Region Settings Guide.

Q8. Setup gives weird errors about not being able to access a folder/file.

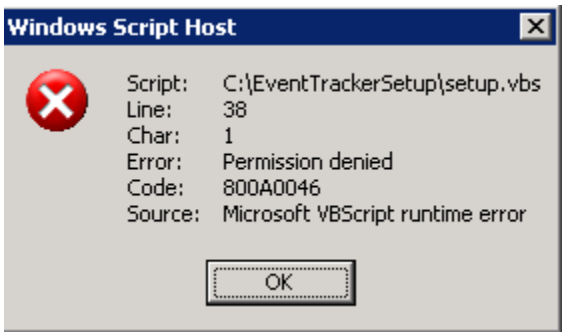


Figure 8

(OR)

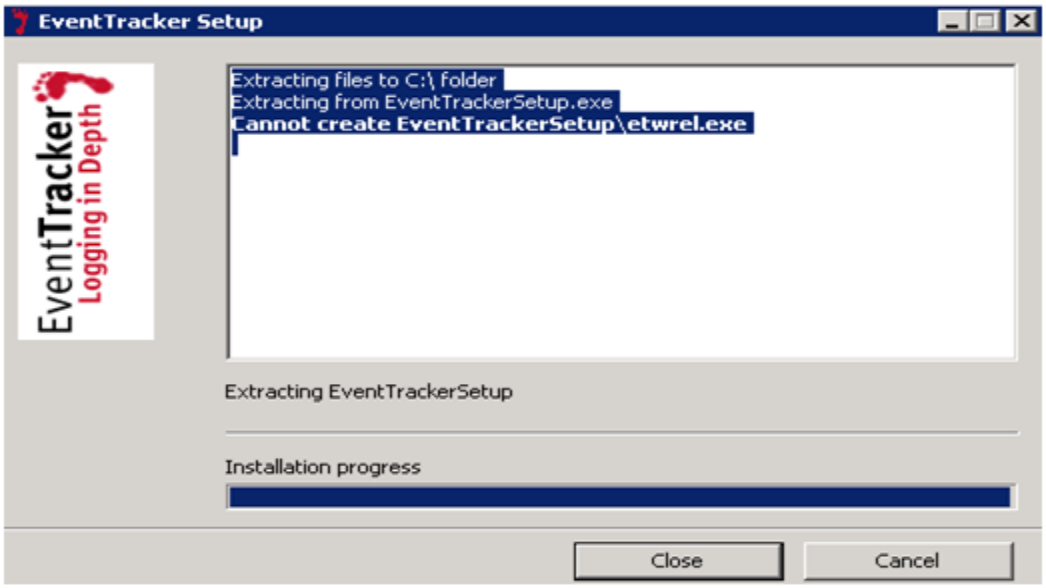


Figure 9

Please make sure that you give a gap of ten seconds for launching the setup. It takes some time for the Operating system to clean up the temporary files/folders created during installation.

Q9. If I get an error message 'You need to format the disk in the drive before you use it. Do you want to format it? ', what should I do?

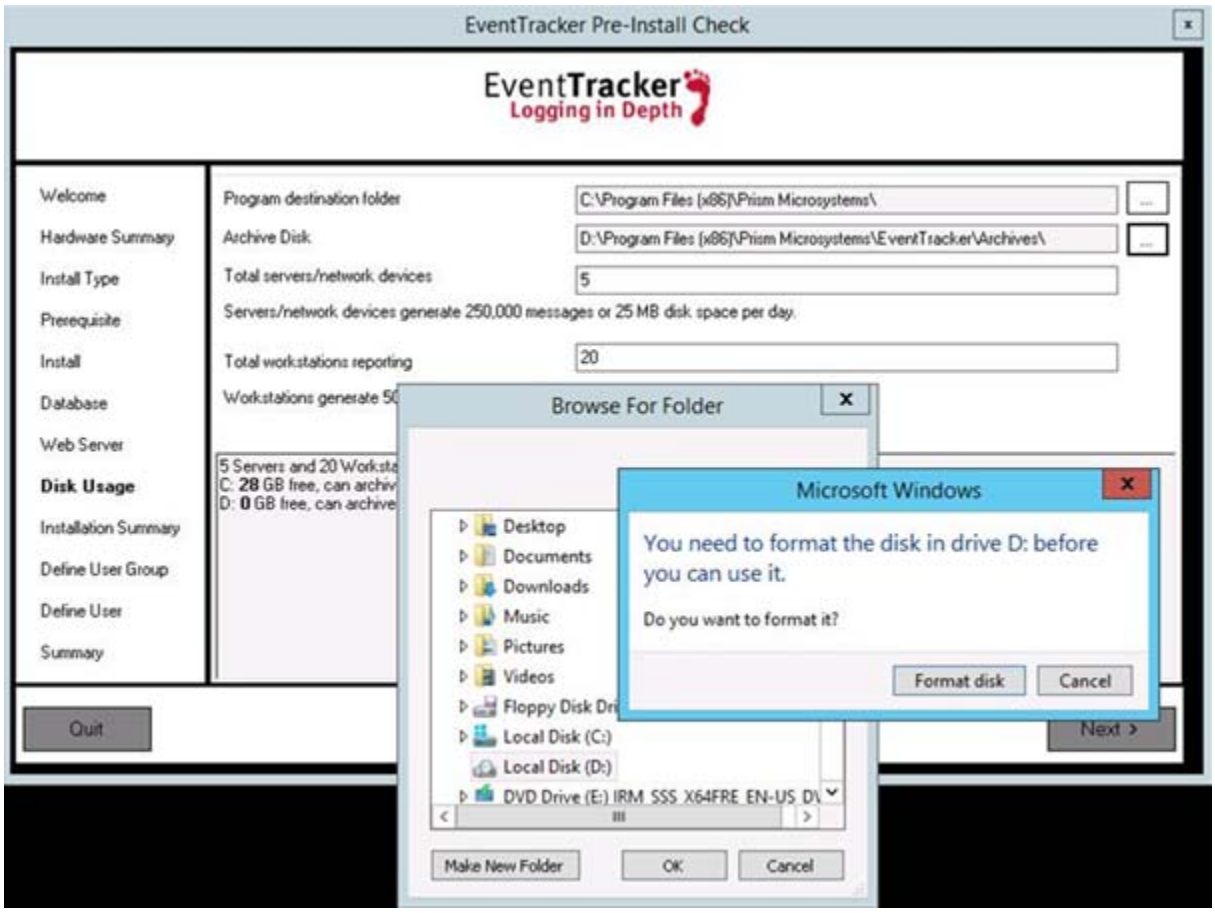


Figure 10

If the setup ends up using an unformatted drive for archive folder, either format the drive for use, or please use a drive that is formatted and is ready for use.

Q10. What should I do, if Microsoft .NET Framework is not installed?

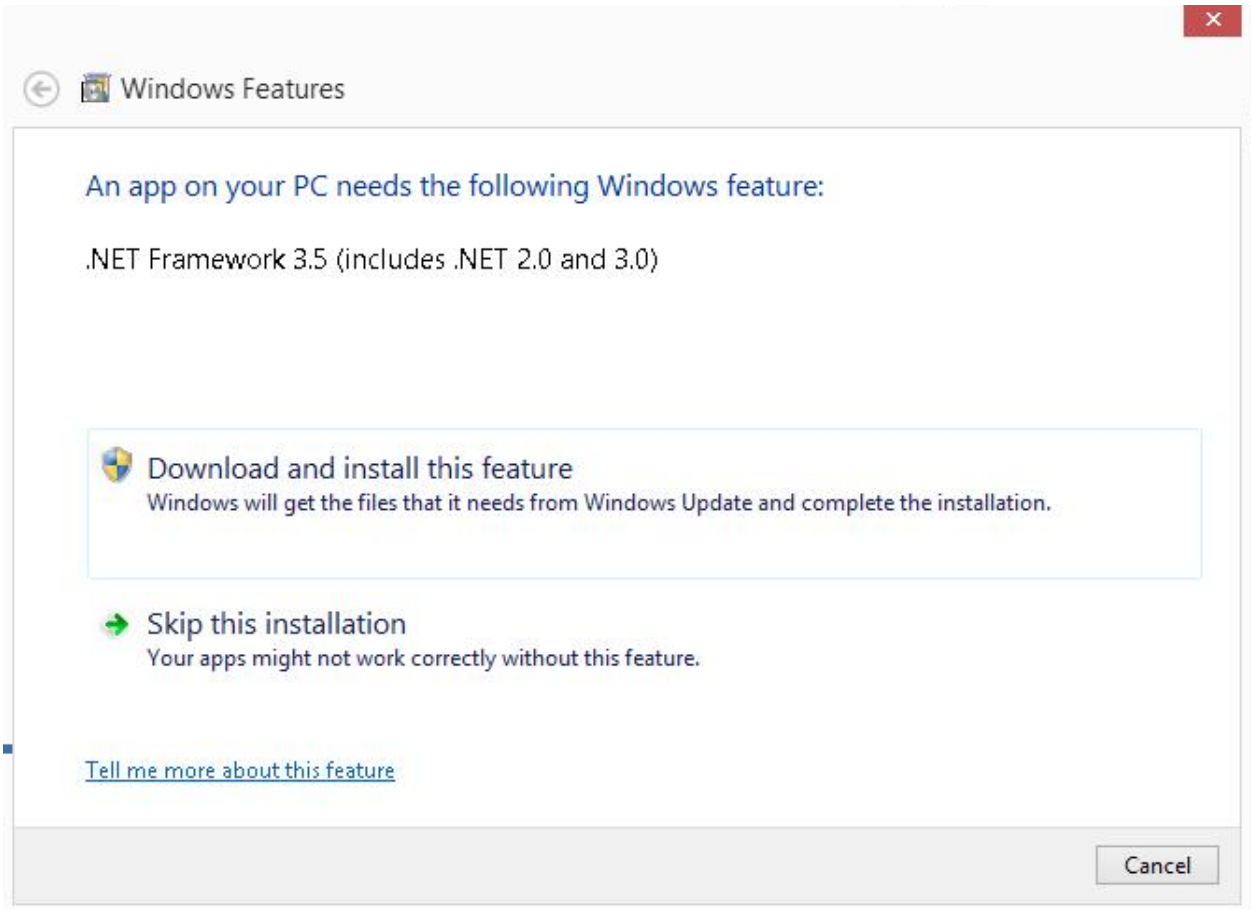

Windows Features
An app on your PC needs the following Windows feature:
.NET Framework 3.5 (includes .NET 2.0 and 3.0)
Download and install this feature
Windows will get the files that it needs from Windows Update and complete the installation.
Skip this installation
Your apps might not work correctly without this feature.
Tell me more about this feature
Cancel

Figure 11

If Microsoft .NET Framework 3.5 is not installed, EventTracker Pre-Install Check displays an appropriate message.

a. Click **Download and Install this feature** and proceed with the installation.

(OR)

If the below message displays,

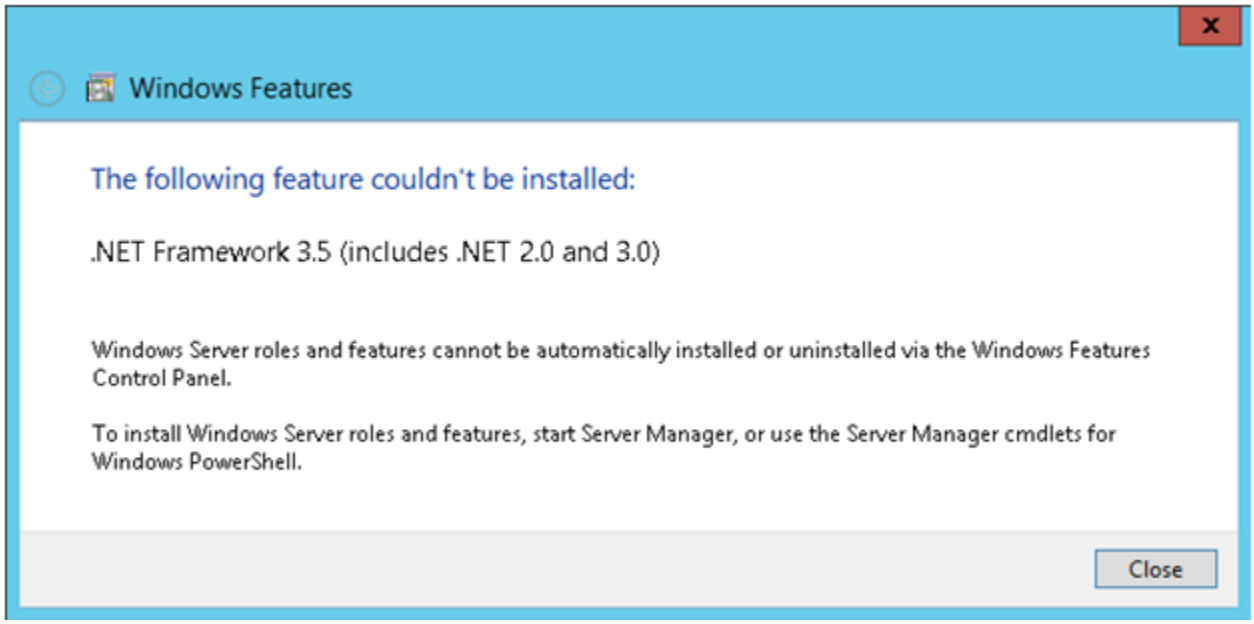

Windows Features
The following feature couldn't be installed:
.NET Framework 3.5 (includes .NET 2.0 and 3.0)
Windows Server roles and features cannot be automatically installed or uninstalled via the Windows Features Control Panel.
To install Windows Server roles and features, start Server Manager, or use the Server Manager cmdlets for Windows PowerShell.
Close

Figure 12

The instructions to install .NET Framework 3.5 is given in detail in How To - Install Microsoft .NET Framework.

Q11. If IIS Express fails to start, then what should I do?

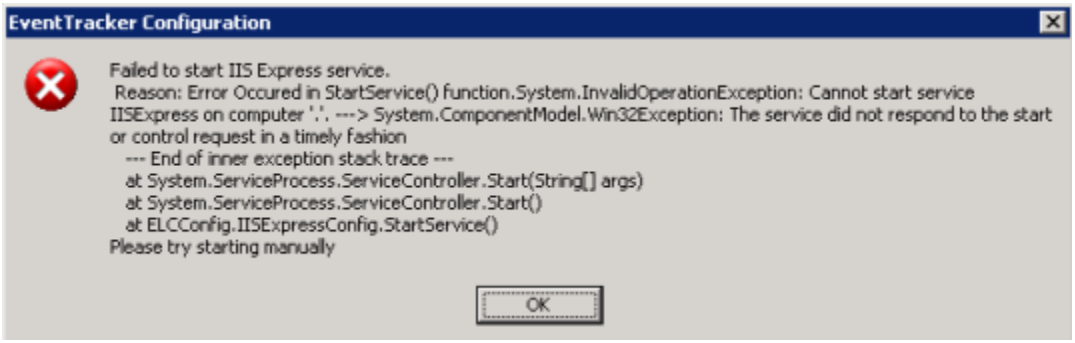

EventTracker Configuration
Failed to start IIS Express service.
Reason: Error Occured in StartService() function.System.InvalidOperationException: Cannot start service IISExpress on computer '.'. ---> System.ComponentModel.Win32Exception: The service did not respond to the start or control request in a timely fashion
--- End of inner exception stack trace ---
at System.ServiceProcess.ServiceController.Start(String[] args)
at System.ServiceProcess.ServiceController.Start()
at ELCConfig.IISExpressConfig.StartService()
Please try starting manually
OK

Figure 13

1. To launch Services Manager, click the **Start** button.
2. In **Search Programs and Files** box, type **Services.msc** and then press **Enter**.

   Services Window displays.
3. Start the service '**IISExpress**' manually.

Q12. If IIS Express failed to install, then what should I do?

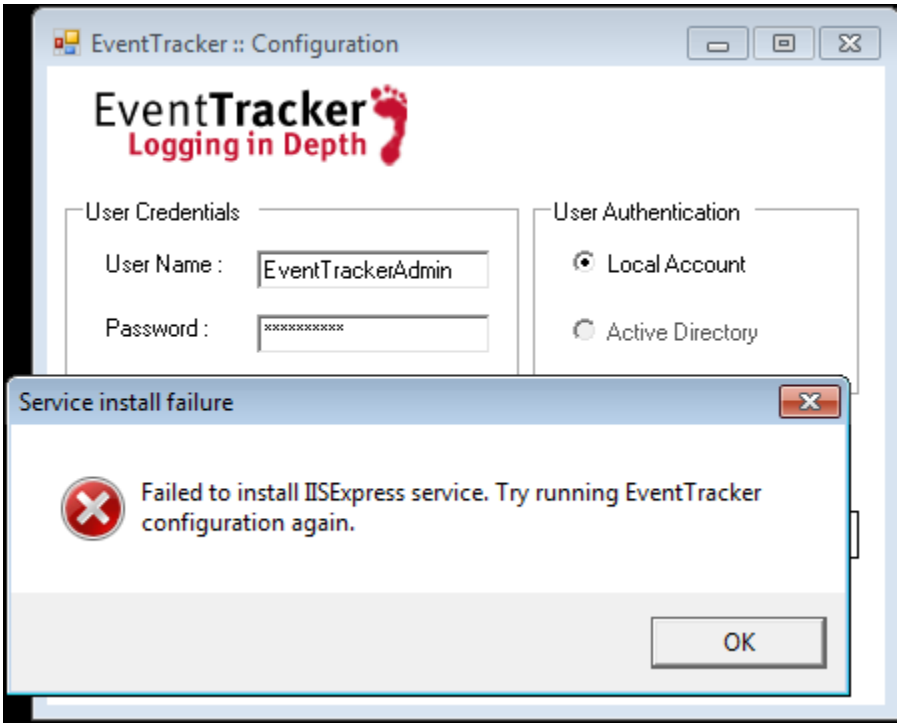


Figure 14

Please run the EventTracker Configuration again.

1. To run EventTracker Configuration, click **Start**, click **Programs**, and then click **Prism Microsystems**.
2. Select **EventTracker**, and then select **EventTracker Configuration**.
3. Enter valid **User Credentials**, and then select the **OK** button.

Q13. How can I use MS SQL Server Enterprise Edition for EventTracker?

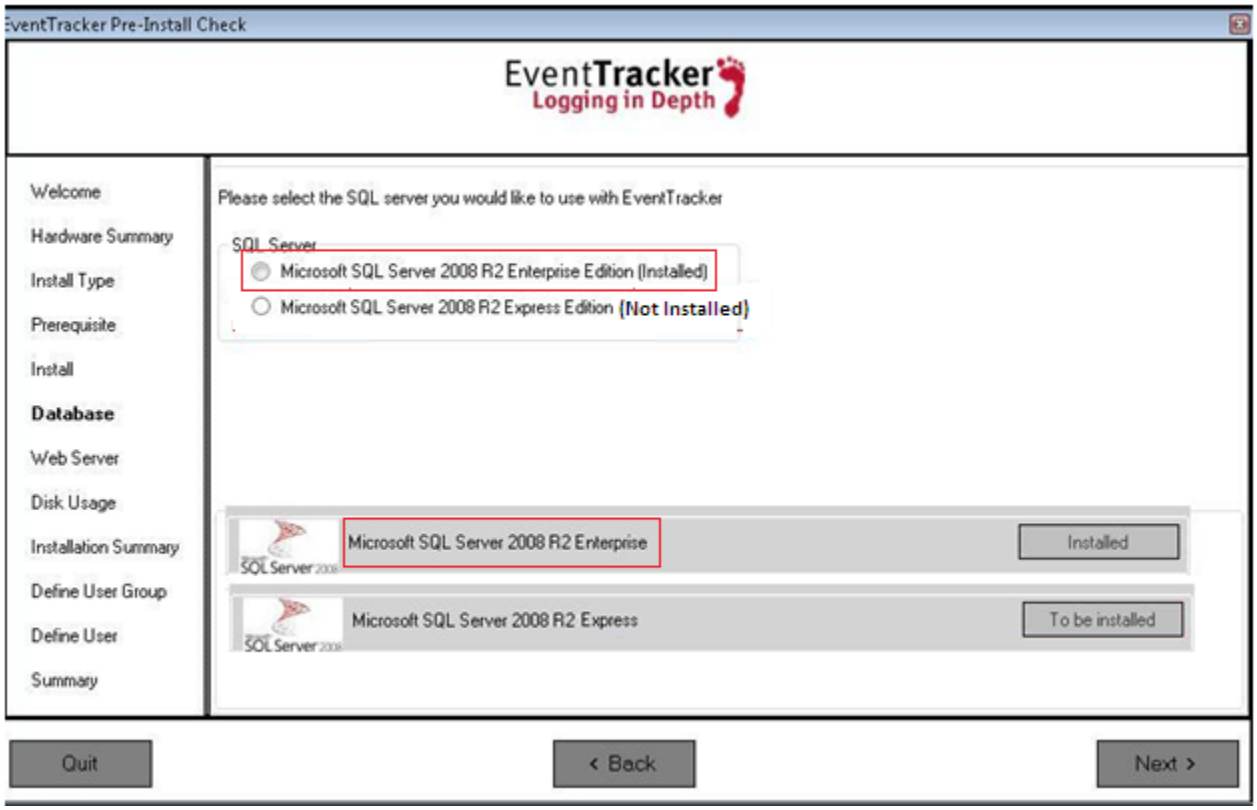


Figure 15

MS SQL Server Enterprise Edition can be used for **Custom** option only. The user can use either SQL Express or Enterprise Edition for **Custom** installation.

SQL Express Edition will be used for Standard and Collection Point Install/Setup Type. The user will be forced to install SQL Express for Standard and Collection Point even if SQL Enterprise Edition is already present on the machine.

System Requirements

For optimal performance, following are the hardware and software requirements to host EventTracker Enterprise.

Hardware Requirements [Min. Configuration]

Minimum hardware required to install and smoothly run EventTracker Enterprise.

32-bit Installation:

CPU	**2GHz, 32-bit (x86) Xeon ® Quad Core or equivalent**
RAM	3 GB
HDD	10 GB Free Hard disk space for the application

Table 1

64-bit Installation:

CPU	**2.80 GHz, 64-bit (x64) Xeon ® Dual Core or equivalent**
RAM	4 GB
HDD	10 GB Free Hard disk space for the application

Table 2

Software Requirements

EventTracker Manager

Windows Platforms	32 bit	64 bit
Server 2012 R2	Not Applicable	Supported
Server 2012	Not Applicable	Supported
Server 2008 R2	Not Applicable	Supported
Server 2008	Supported	Supported
Server 2003 R2	Supported	Supported
Server 2003	Supported	Supported

Table 3

Components:

- Microsoft .NET Framework 3.5 SP1.

- Microsoft SQL SERVER 2005/2008/2008 R2/2012/2012 R2 – Express/Enterprise /Standard Edition.
- IIS 6.0 and above. Also IIS Express is supported on v7.5 Build 53 and above (**except Win 2003 64 bit OS, Vista 64 bit OS**).

Web Browsers:

- Internet Explorer 8.0 and above
- Firefox Browser 3.5 and above

Note: EventTracker Enterprise installation on Windows 2012/2012 R2/2008/2008 R2 Server Core edition not supported.

EventTracker Agent

Windows Platforms	32 bit	64 bit
Server 2012 R2	Not Applicable	Supported
Server 2012	Not Applicable	Supported
Server 2008 R2	Not Applicable	Supported
Server 2008	Supported	Supported
Server 2003 R2	Supported	Supported
Server 2003	Supported	Supported
Windows 7	Supported	Supported
2000 Server	Supported	Supported
Windows XP	Supported	Supported
2000 Professional	Supported	Supported
Windows 8, 8.1	Supported	Supported
Vista	Supported	Supported
EventTracker Agent for Solaris: Solaris 9, Solaris 10		

Table 4

Components:

- Microsoft .NET Framework 2.0 and above.

NOTE: Versions other than those specified above are not supported.

Pre-install instructions for Local Account and Active Directory authentication v7.5.29 and below versions

- EventTracker Enterprise users are authenticated locally or against the Windows Active Directory.
- If you want 'Local Account' authentication, then user accounts and group accounts should preexist on the target computer where EventTracker Enterprise is to be installed. So, create user accounts and group accounts on the target computer before you attempt to install EventTracker Enterprise.
- If you want 'Active Directory' authentication, then user accounts and group accounts should preexist in the Active Directory. So, create user accounts and group accounts in the Active Directory before you attempt to install EventTracker Enterprise.

Create Local User and Group Accounts

NOTE:

To perform this procedure, you must be a member of the administrators group on the local computer, or you must have been delegated the appropriate authority. If the computer is joined to a domain, then members of the 'Local Admin' group might be able to perform this procedure.

Summary

- What is the significance of creating 'EventTracker' user group?
  - √ To log on to EventTracker Enterprise, the user must be a member of 'EventTracker' group.
  - √ EventTracker Enterprise user authentication operates locally, that is confined to a particular computer or within Active Directory context.

- Create a local user group 'EventTracker**' on the computer where EventTracker Enterprise is to be installed.
  - √ Create a local user e.g. ETKaren**.
  - √ Add ETKaren user to EventTracker group. Members of this group can log on to EventTracker Enterprise.

√ Add ETKaren user to local Administrators group on the computer where EventTracker Enterprise is to be installed.

*** You can name user group and user with any name you prefer and need not necessarily be EventTracker and ETKaren.

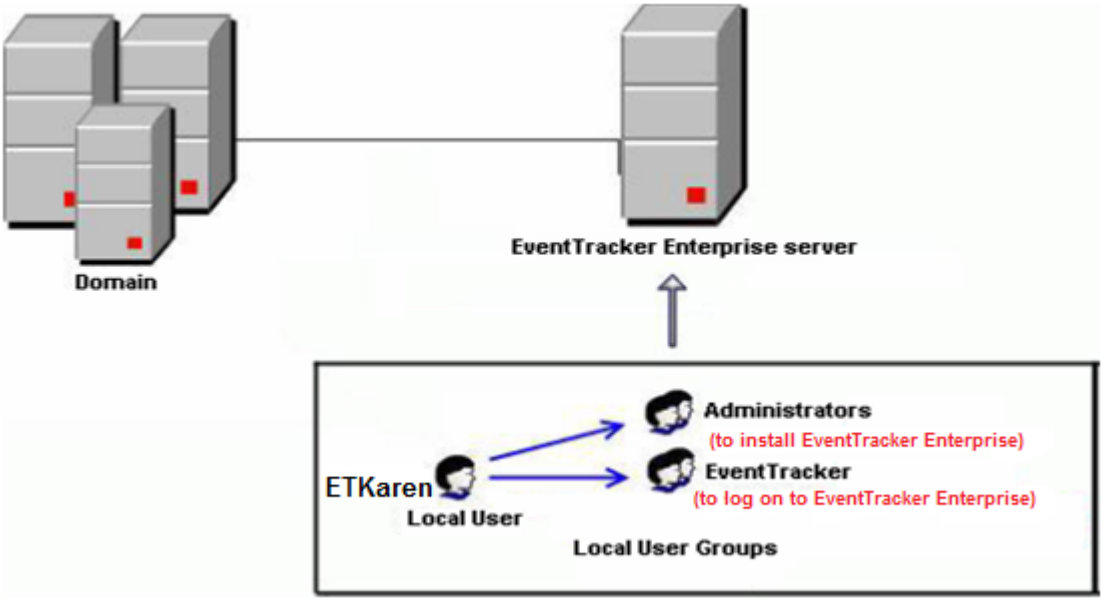


Figure 16

Create EventTracker User Group

1. Select the **Start** button, select **Control Panel**, and then select **Administrative Tools**.
2. Select **Computer Management**, and then select **Local Users and Groups**.

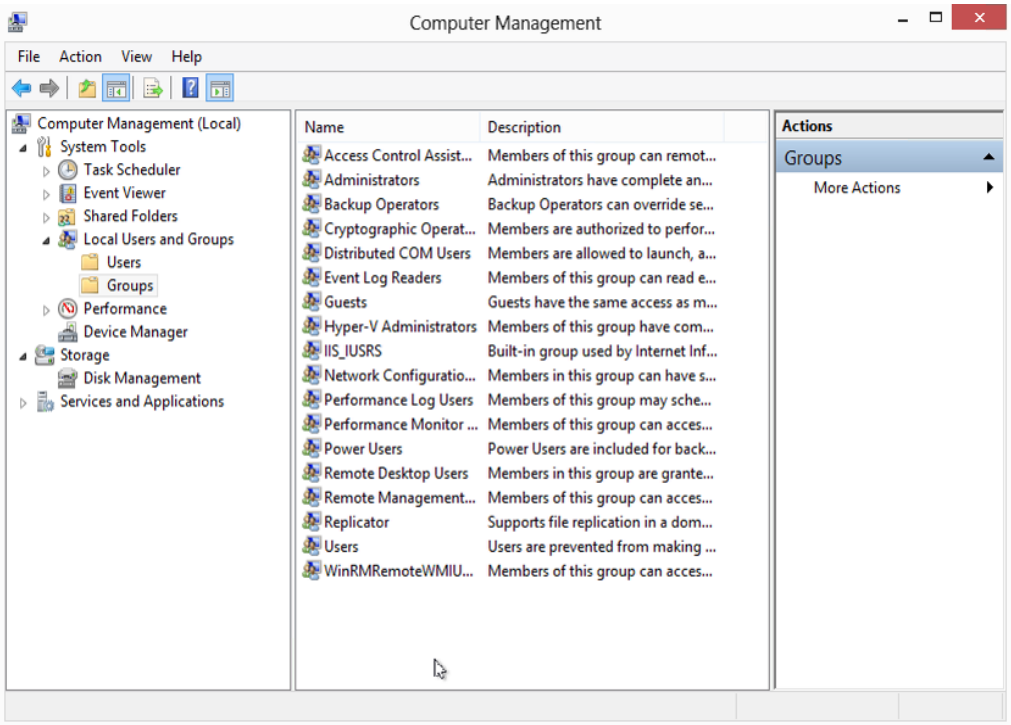

Computer Management
File Action View Help
Computer Management (Local)
System Tools
Task Scheduler
Event Viewer
Shared Folders
Local Users and Groups
Users
Groups
Performance
Device Manager
Storage
Disk Management
Services and Applications
Name
Description
Access Control Assist... Members of this group can remot...
Administrators Administrators have complete an...
Backup Operators Backup Operators can override se...
Cryptographic Operat... Members are authorized to perfor...
Distributed COM Users Members are allowed to launch, a...
Event Log Readers Members of this group can read e...
Guests Guests have the same access as m...
Hyper-V Administrators Members of this group have com...
IIS_IUSRS Built-in group used by Internet Inf...
Network Configuratio... Members in this group can have s...
Performance Log Users Members of this group may sche...
Performance Monitor ... Members of this group can acces...
Power Users Power Users are included for back...
Remote Desktop Users Members in this group are grante...
Remote Management... Members of this group can acces...
Replicator Supports file replication in a dom...
Users Users are prevented from making ...
WinRMRemoteWMIU... Members of this group can acces...
Actions
Groups
More Actions

Figure 17

3. Expand the **Local Users and Groups** node. Right – click **Groups,** and then select **New Group.**

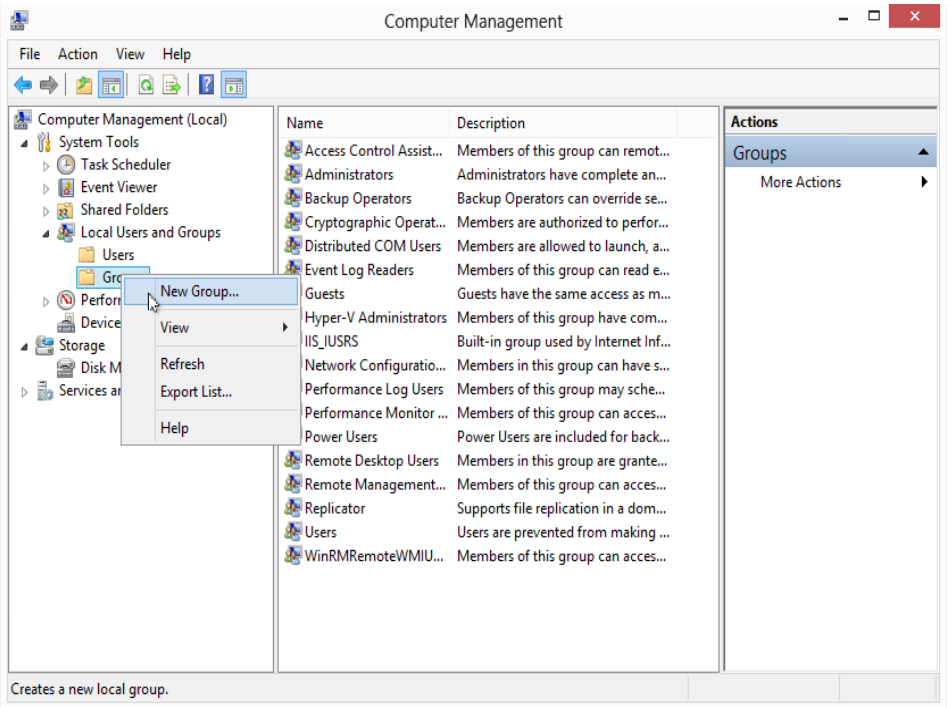

Computer Management
File Action View Help
Computer Management (Local)
System Tools
Task Scheduler
Event Viewer
Shared Folders
Local Users and Groups
Users
Groups
Performance
Device Manager
Storage
Disk Management
Services and Applications
New Group...
View
Refresh
Export List...
Help
Name
Description
Access Control Assist... Members of this group can remot...
Administrators Administrators have complete an...
Backup Operators Backup Operators can override se...
Cryptographic Operat... Members are authorized to perfor...
Distributed COM Users Members are allowed to launch, a...
Event Log Readers Members of this group can read e...
Guests Guests have the same access as m...
Hyper-V Administrators Members of this group have com...
IIS_IUSRS Built-in group used by Internet Inf...
Network Configuratio... Members in this group can have s...
Performance Log Users Members of this group may sche...
Performance Monitor ... Members of this group can acces...
Power Users Power Users are included for back...
Remote Desktop Users Members in this group are grante...
Remote Management... Members of this group can acces...
Replicator Supports file replication in a dom...
Users Users are prevented from making ...
WinRMRemoteWMIU... Members of this group can acces...
Actions
Groups
More Actions
Creates a new local group.

Figure 18

4. Type the name of the group in the **Group name** field.

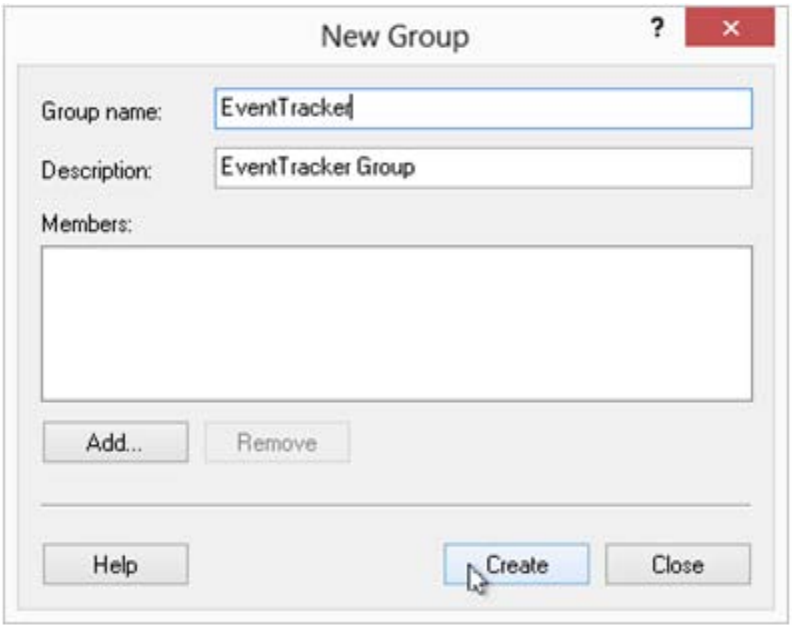


Figure 19

5. Select **Create**, and then select **Close.**

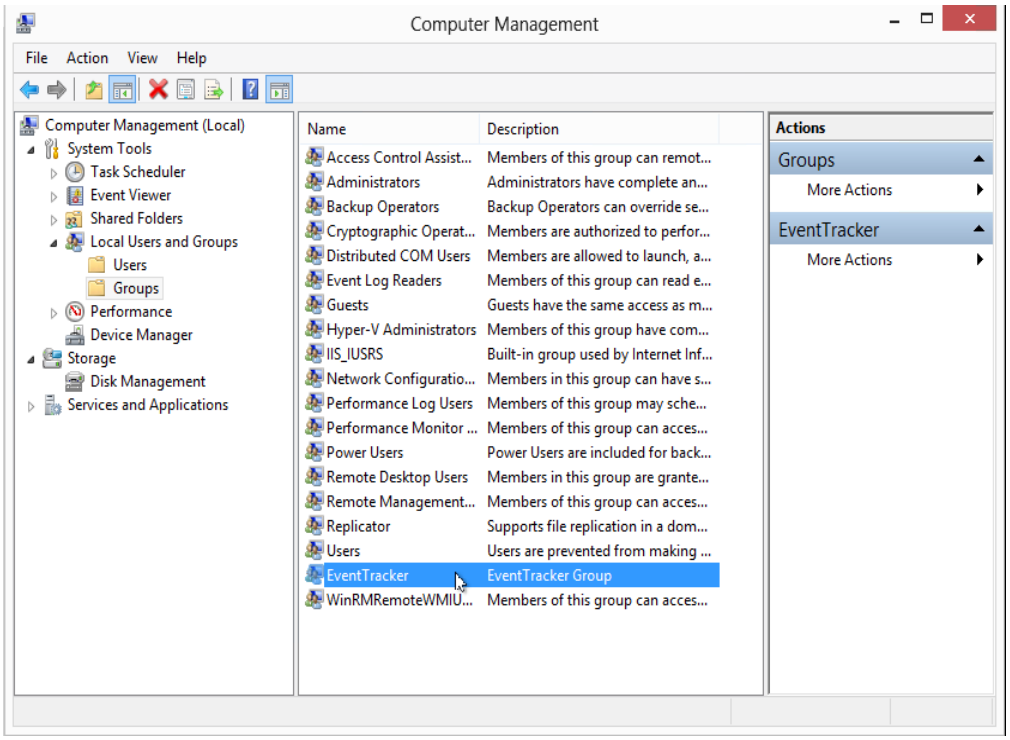

Computer Management
File Action View Help
Computer Management (Local)
System Tools
Task Scheduler
Event Viewer
Shared Folders
Local Users and Groups
Users
Groups
Performance
Device Manager
Storage
Disk Management
Services and Applications
Name
Description
Access Control Assist... Members of this group can remot...
Administrators Administrators have complete an...
Backup Operators Backup Operators can override se...
Cryptographic Operat... Members are authorized to perfor...
Distributed COM Users Members are allowed to launch, a...
Event Log Readers Members of this group can read e...
Guests Guests have the same access as m...
Hyper-V Administrators Members of this group have com...
IIS_IUSRS Built-in group used by Internet Inf...
Network Configuratio... Members in this group can have s...
Performance Log Users Members of this group may sche...
Performance Monitor ... Members of this group can acces...
Power Users Power Users are included for back...
Remote Desktop Users Members in this group are grante...
Remote Management... Members of this group can acces...
Replicator Supports file replication in a dom...
Users Users are prevented from making ...
EventTracker EventTracker Group
WinRMRemoteWMIU... Members of this group can acces...
Actions
Groups
More Actions
EventTracker
More Actions

Figure 20

EventTracker group is created.

Create User

1. In **Local Users and Groups** node, right-click **Users**, and then select **New User**.

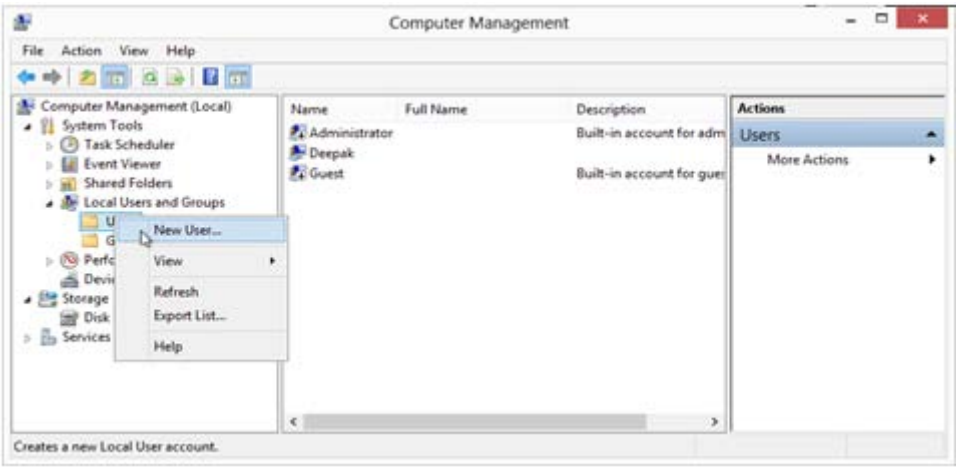


Figure 21

2. Type appropriate user credentials.

   For example, you can type 'ETKaren' as user name.

3. Provide a strong password and confirm the same.
4. Select the **Password never expires** check box.

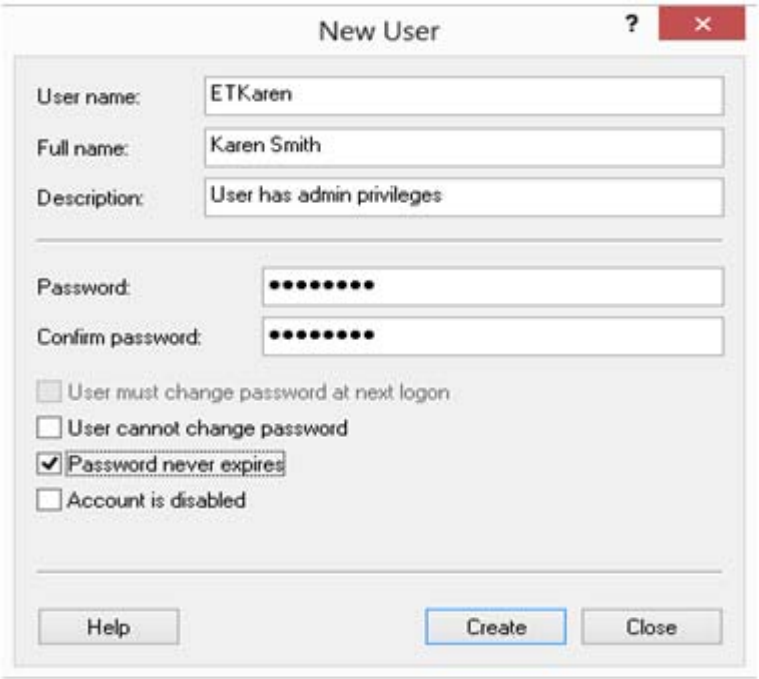


Figure 22

NOTE:

It is not mandatory to check **Password never expires** option. In order to avoid password expiry of EventTracker every now and then, we recommend you to check this option.

5. Select **Create**, and then select **Close.**

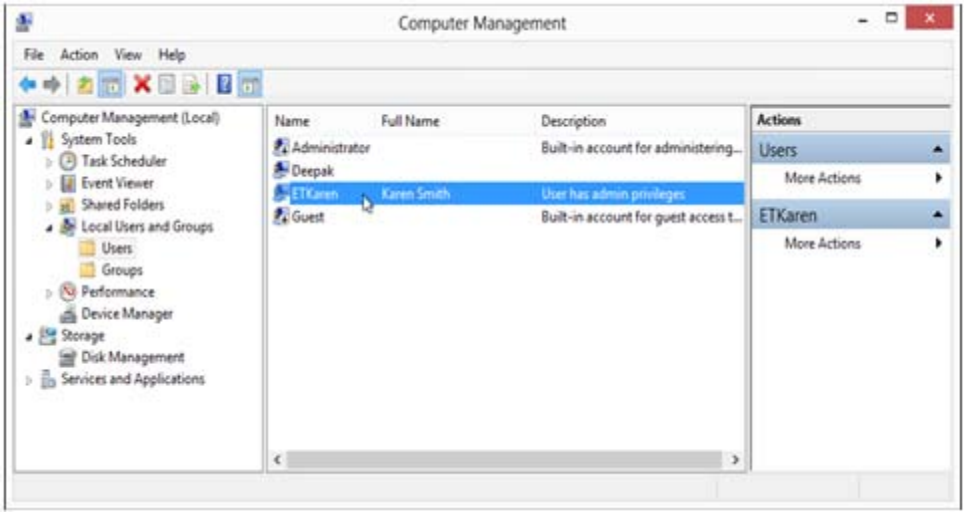


Figure 23

ETKaren user is created.

Add User to EventTracker Group

1. Right-click the newly created user group, and then select **Properties.**

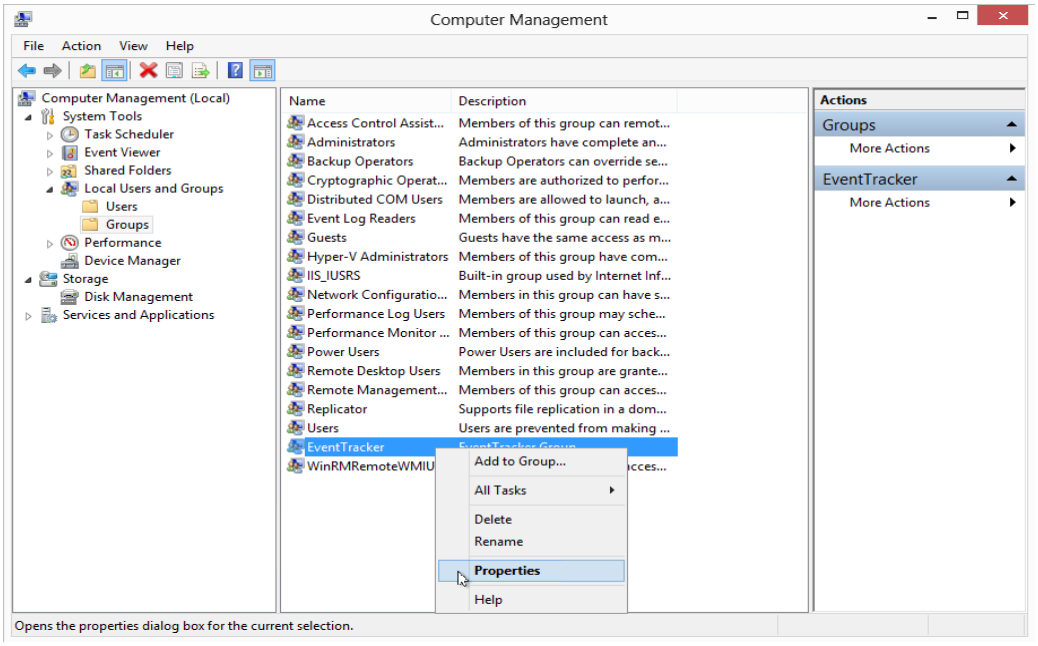


Figure 24

EventTracker Properties window displays.

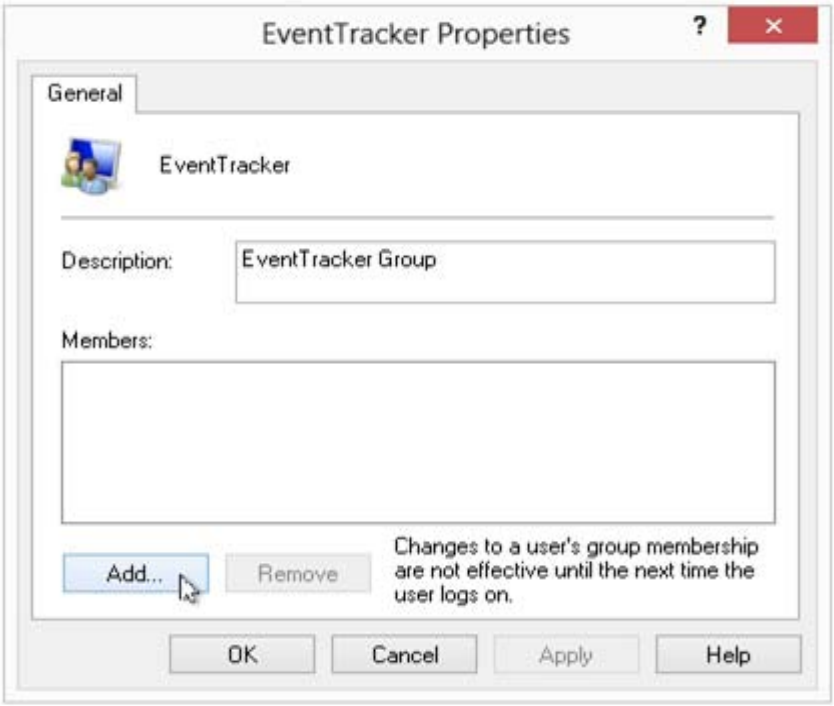


Figure 25

2. Select the **Add** button.

   Select Users, Computers, Service Accounts or Groups window displays.

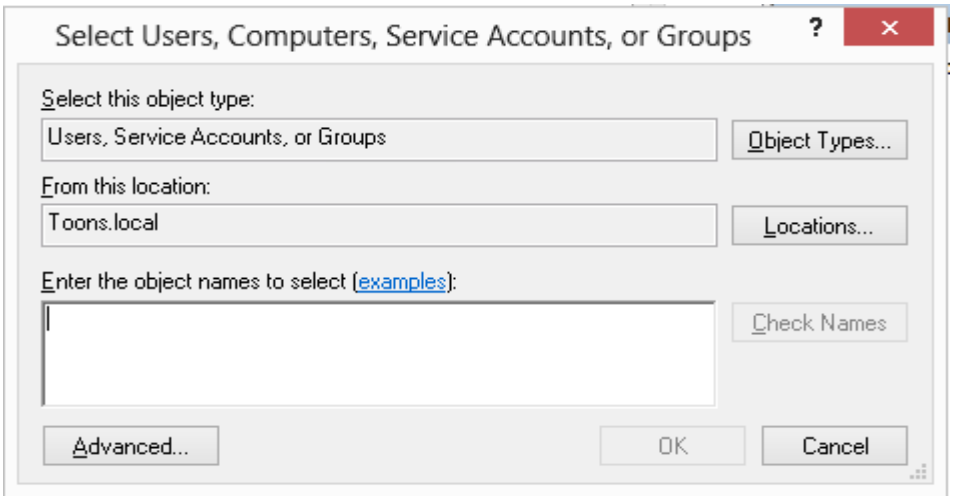


Figure 26

3. Select the **Locations** button.

   Locations window displays.

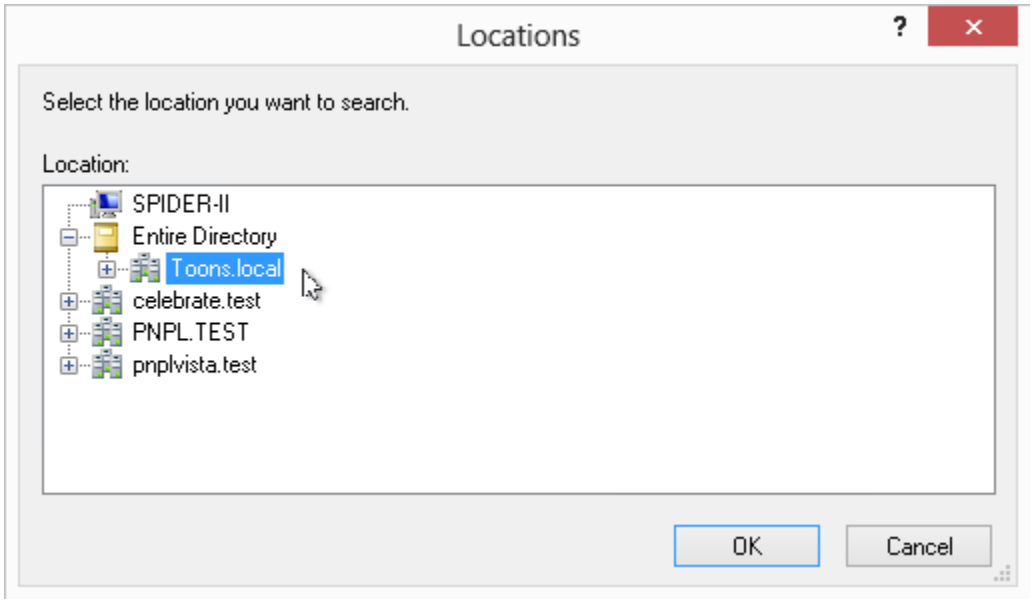


Figure 27

4. Select the location, typically the name of the computer.

   In this example, name of the computer is SPIDER-II. Refer Figure 13.

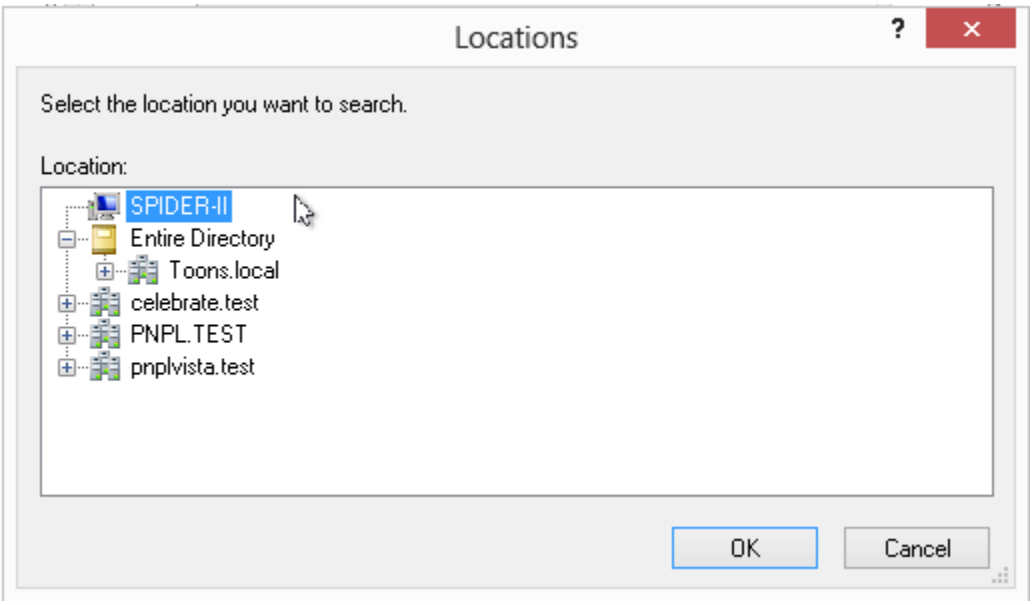


Figure 28

5. Select the **OK** button.

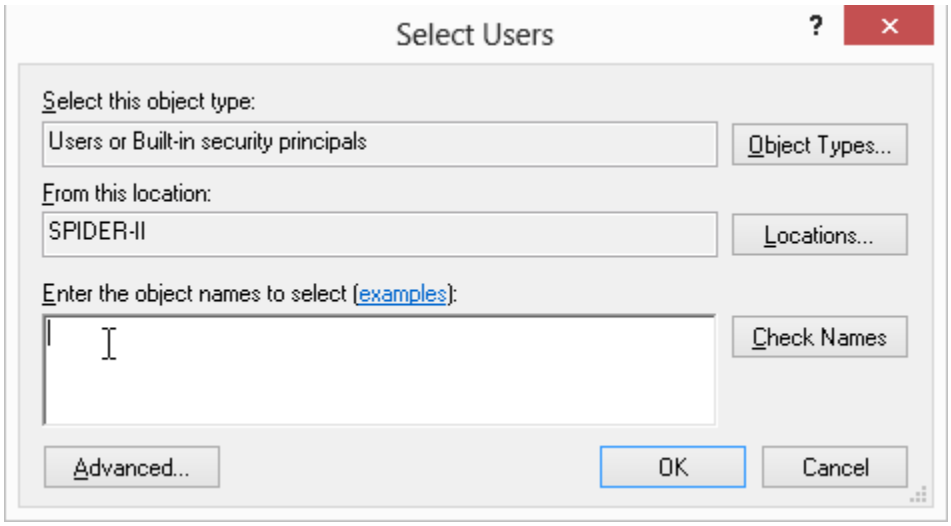


Figure 29

6. Type the user name in the **Enter the object names to select** field.

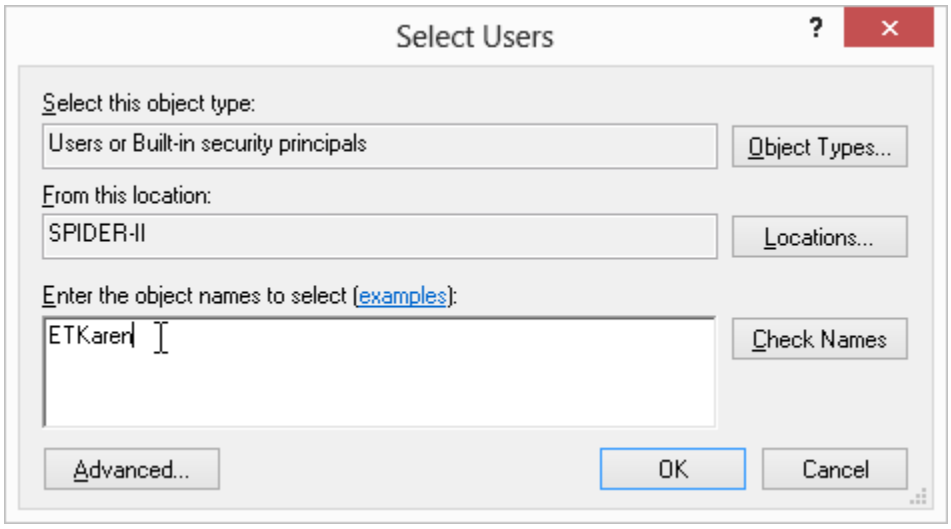


Figure 30

7. Select the **Check Names** button**.**

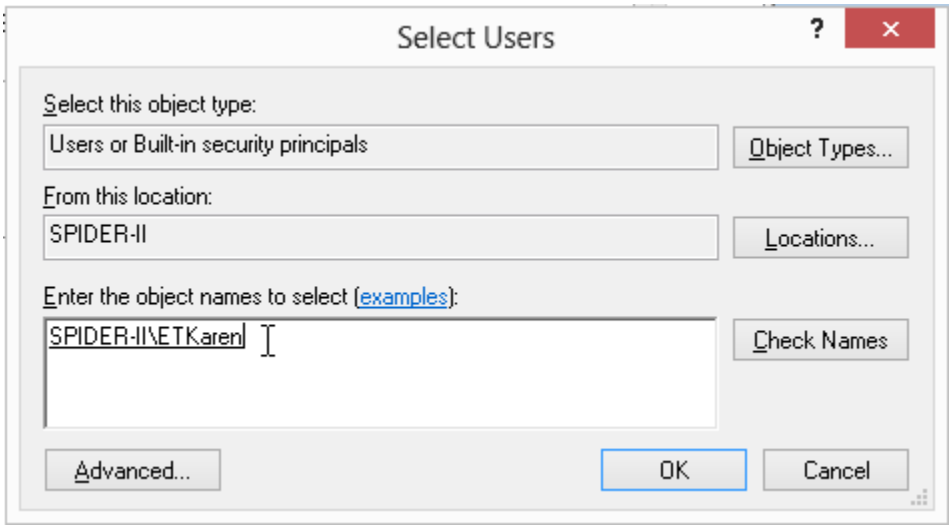


Figure 31

8. Select the **OK** button**.**

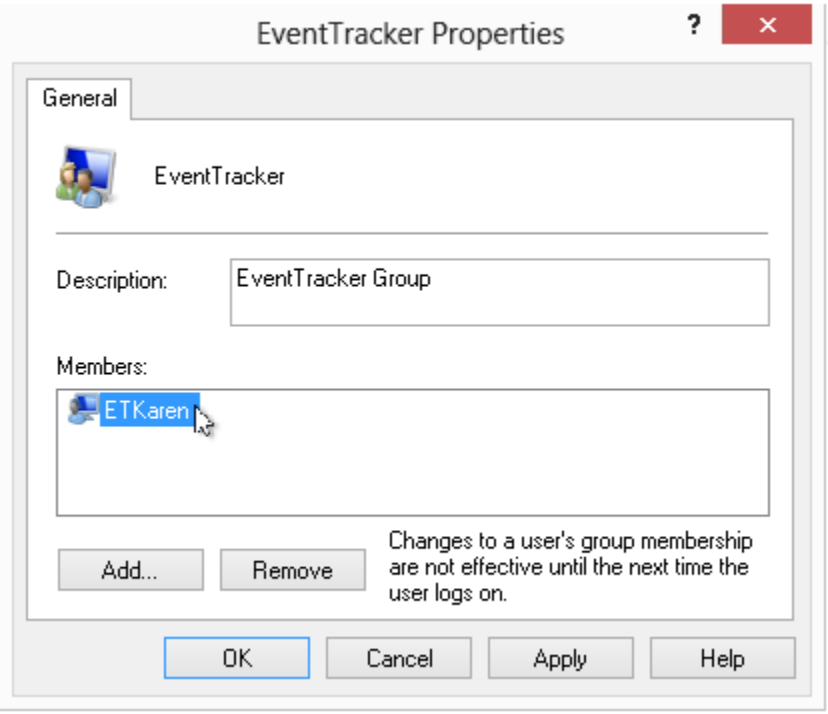


Figure 32

9. Select **Apply,** and then select the **OK** button**.**

Create Active Directory User and Group Accounts

NOTE:

To perform this procedure, you must be a member of the 'Account Operators' group, 'Local Admin' group, or the 'Enterprise Admin' group in Active Directory, or you must have been delegated the appropriate authority.

Summary:

a. Create a user group e.g. EventTracker Test** in the domain where EventTracker Enterprise is to be installed.
b. Create a domain user e.g. ETKaren**.

   Add ETKaren user to EventTracker Test group. Members of this group can log on to EventTracker Enterprise.

c. Add ETKaren user to local Administrators group on the computer where EventTracker Enterprise is to be installed.

   ** You can name user group and user with any name you prefer and need not necessarily be EventTracker Test and ETKaren.

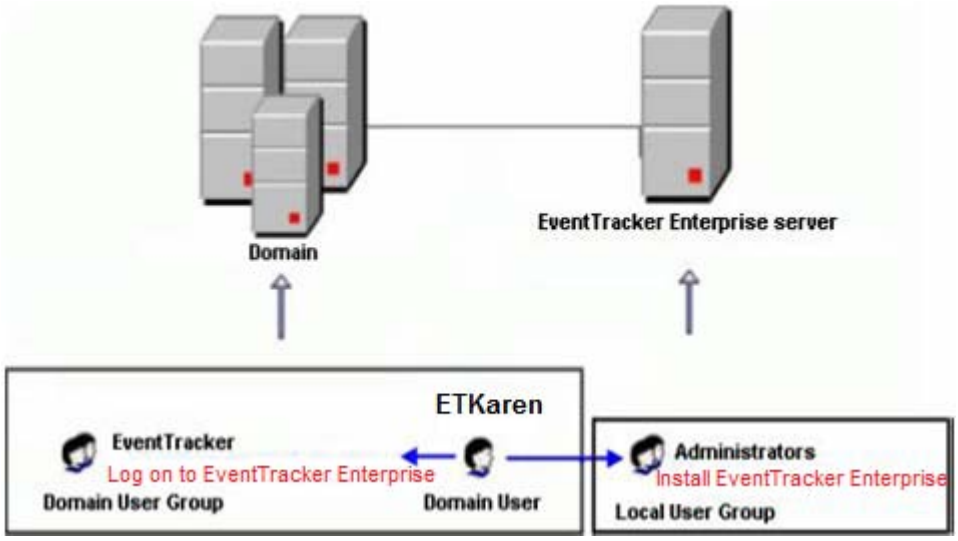


Figure 33

Create EventTracker Group

1. Select the **Start** button, select **Settings**, and then select **Control Panel.**

2. Select **Administrative Tools**, and then select **Active Directory Users and Computers**.

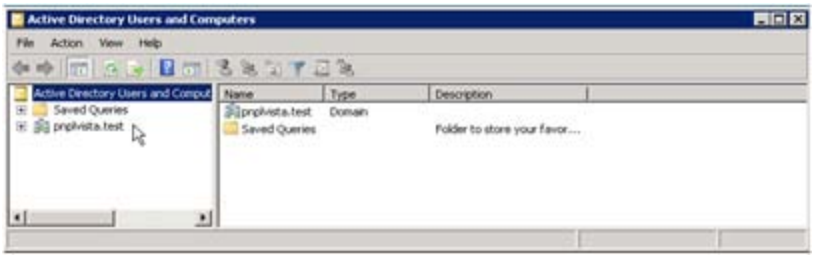


Figure 34

Create a **Global Scope Security Group** in the domain where EventTracker Enterprise is to be installed.

3. Right-click the domain name, select **New**, and then select **Group**.

In this example, domain name is 'pnplvista.test'.

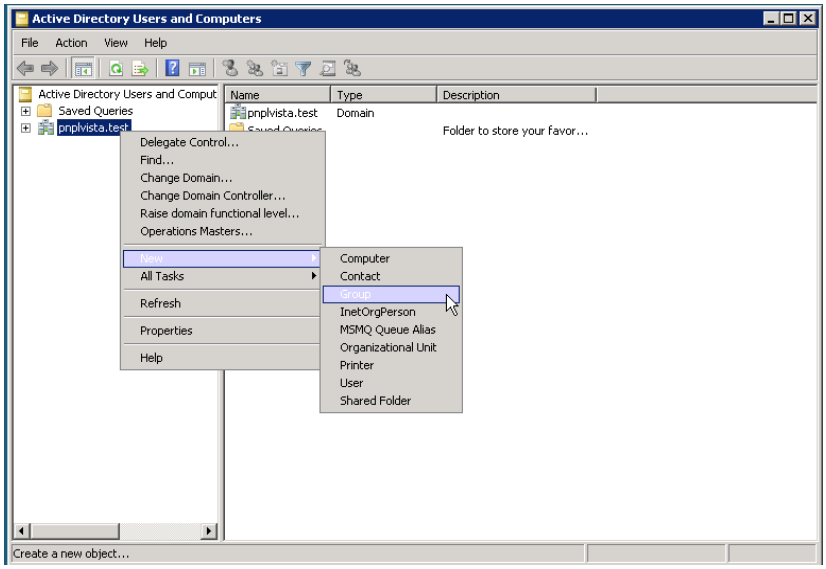


Figure 35

New Object – Group displays.

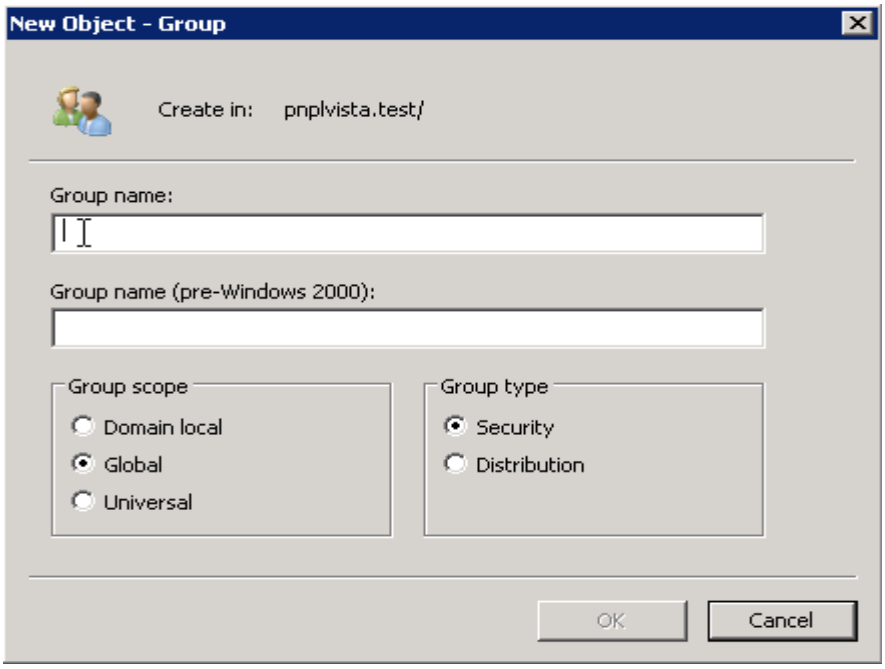


Figure 36

4. Type the name of the group in the **Group name** field.

   In this example group name is 'EventTracker Test'.

5. Select **Group scope** as **Global**, and **Group type** as **Security**.

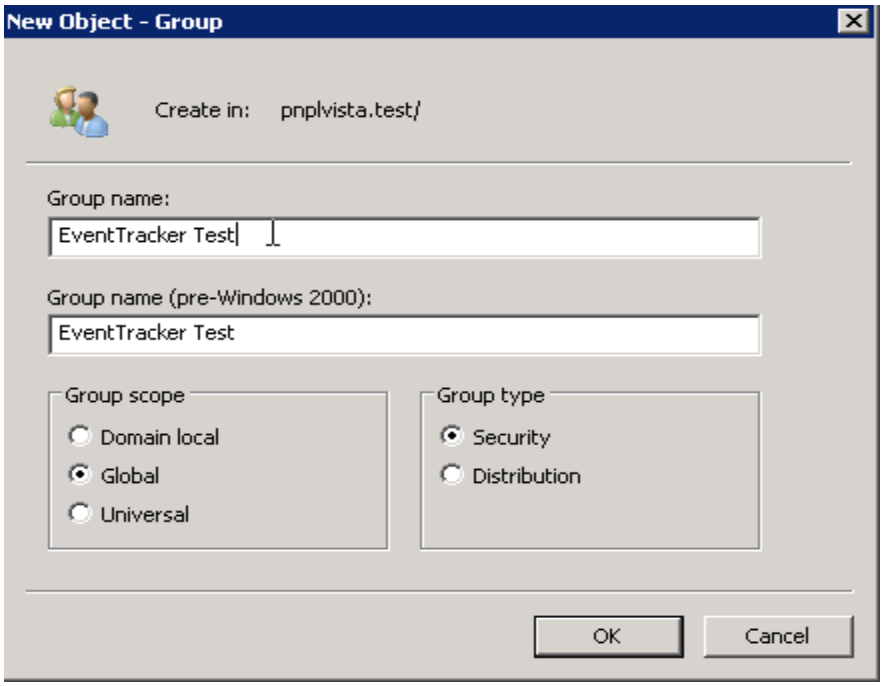


Figure 37

6. Click **OK.**

'EventTracker Test' group is created.

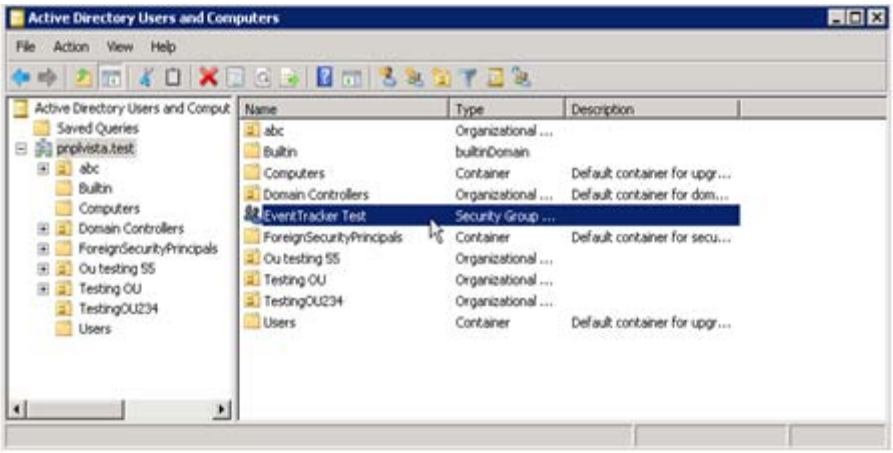


Figure 38

Create User

1. Right-click **Users**, point to **New**, and then **User**.

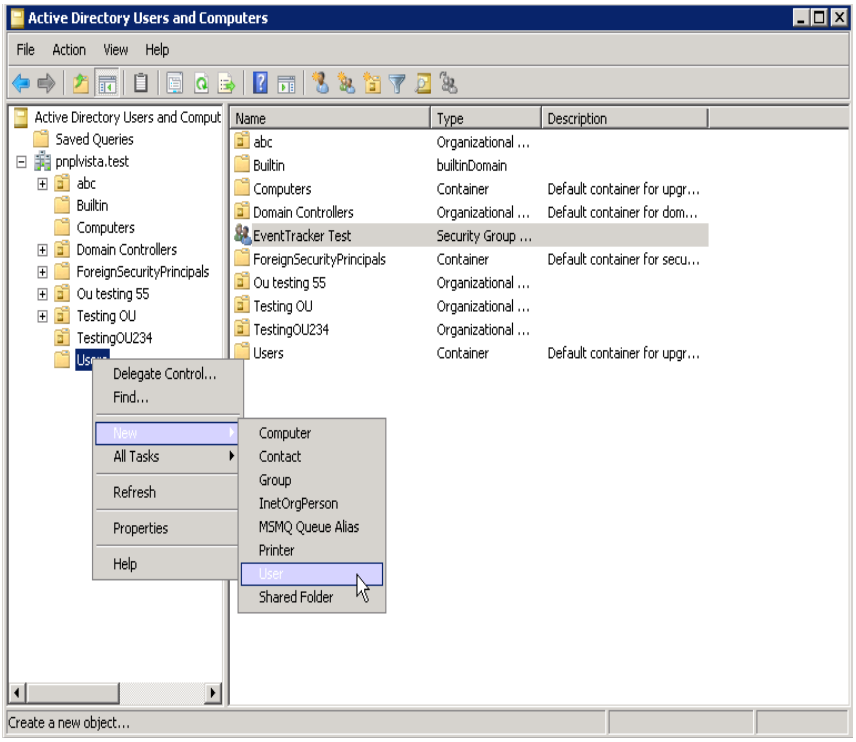


Figure 39

New Object – User window displays.

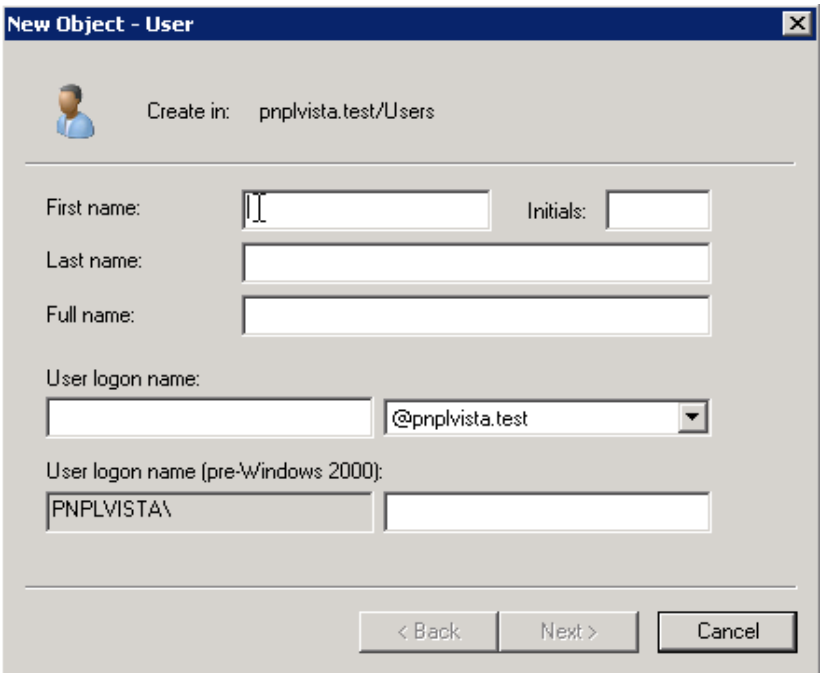


Figure 40

2. Type appropriately in the respective fields.

   In this example, First name is 'Karen', Last name is 'Smith' and User logon name is 'ETKaren'.

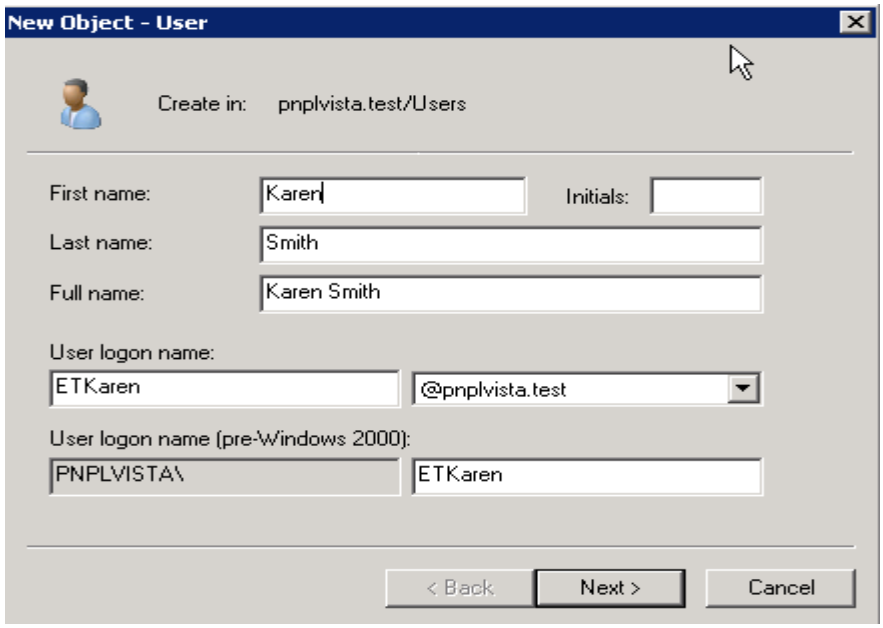


Figure 41

3. Select the **Next >** button.

4. Type the password in the **Password** and **Confirm Password** fields.

5. Select the **Password Never Expires** check box.

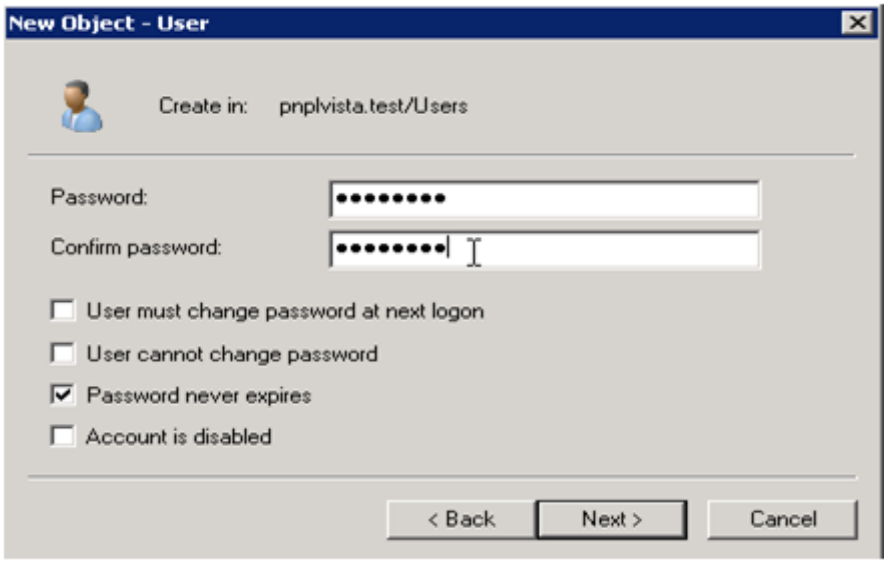


Figure 42

NOTE:
It is not mandatory to check **Password never expires** option. In order to avoid password expiry of EventTracker every now and then, we recommend you to check this option.

6. Select the **Next** > button.

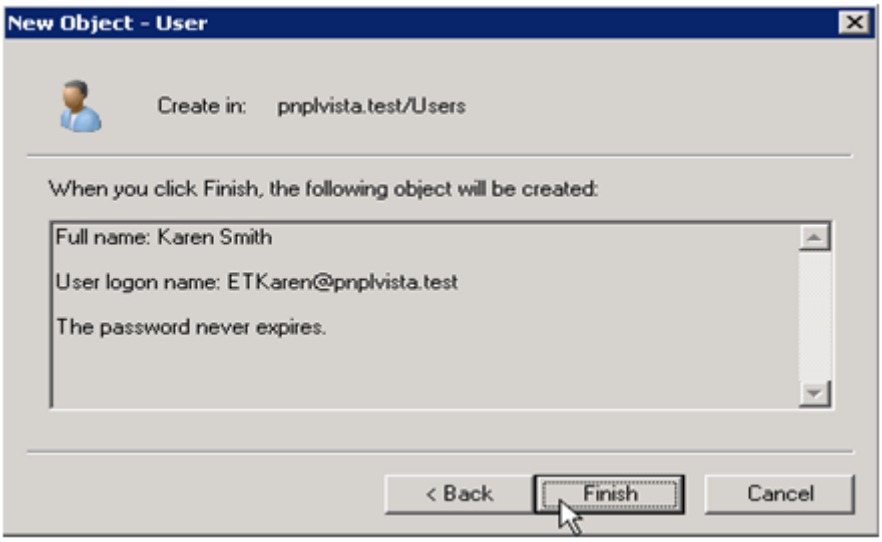


Figure 43

7. Select the **Finish** button.

Username 'Karen Smith' is created.

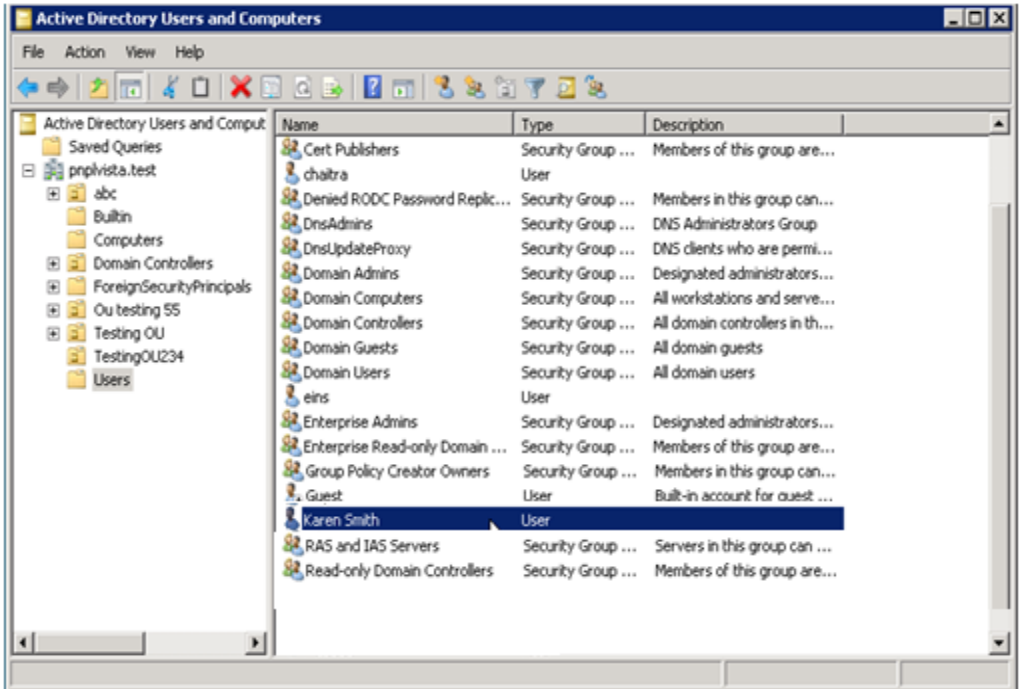

Active Directory Users and Computers
File Action View Help
Active Directory Users and Comput
Saved Queries
pnplvista.test
abc
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Ou testing 55
Testing OU
TestingOU234
Users
Name Type Description
Cert Publishers Security Group ... Members of this group are...
chaitra User
Denied RODC Password Replic... Security Group ... Members in this group can...
DnsAdmins Security Group ... DNS Administrators Group
DnsUpdateProxy Security Group ... DNS clients who are permi...
Domain Admins Security Group ... Designated administrators...
Domain Computers Security Group ... All workstations and serve...
Domain Controllers Security Group ... All domain controllers in th...
Domain Guests Security Group ... All domain guests
Domain Users Security Group ... All domain users
eins User
Enterprise Admins Security Group ... Designated administrators...
Enterprise Read-only Domain ... Security Group ... Members of this group are...
Group Policy Creator Owners Security Group ... Members in this group can...
Guest User Built-in account for guest ...
Karen Smith User
RAS and IAS Servers Security Group ... Servers in this group can ...
Read-only Domain Controllers Security Group ... Members of this group are...

Figure 44

Add User to EventTracker Group

1. Right-click the **EventTracker Test** group, and then select **Properties**.

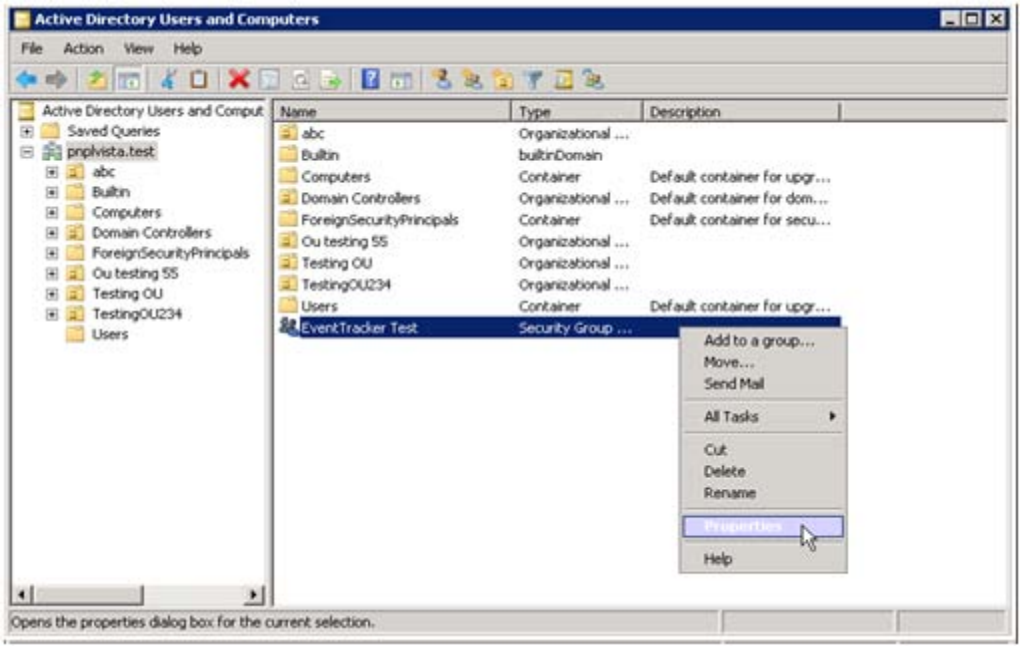


Figure 45

EventTracker Properties window displays.

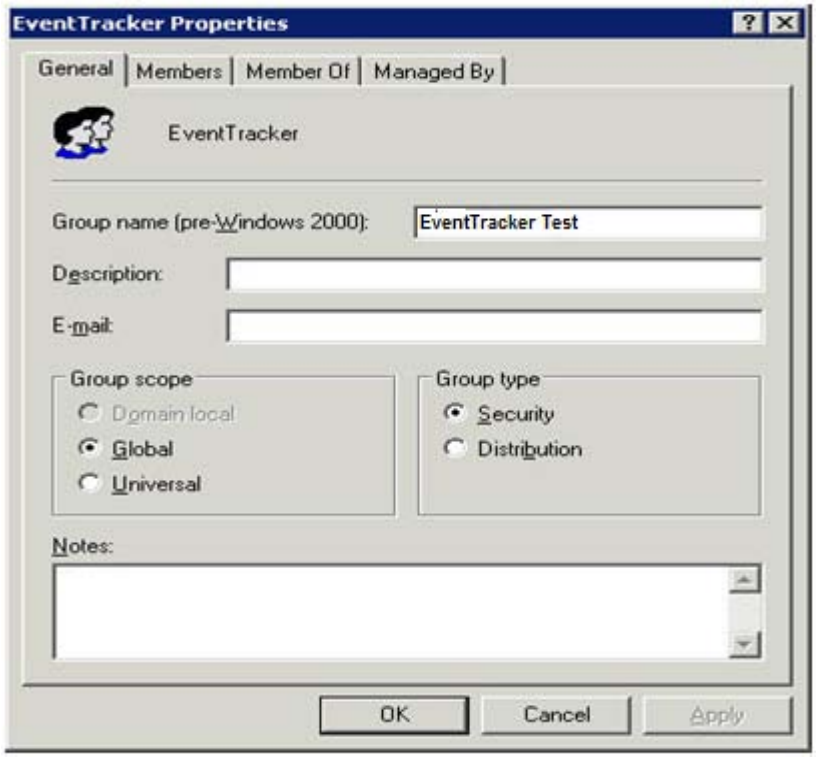


Figure 46

2. Select the **Members** tab.

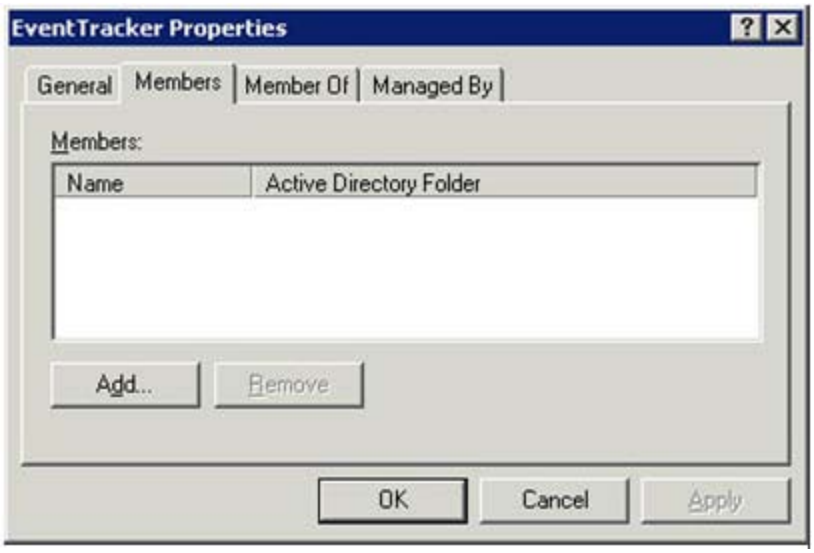


Figure 47

3. Select the **Add** button.

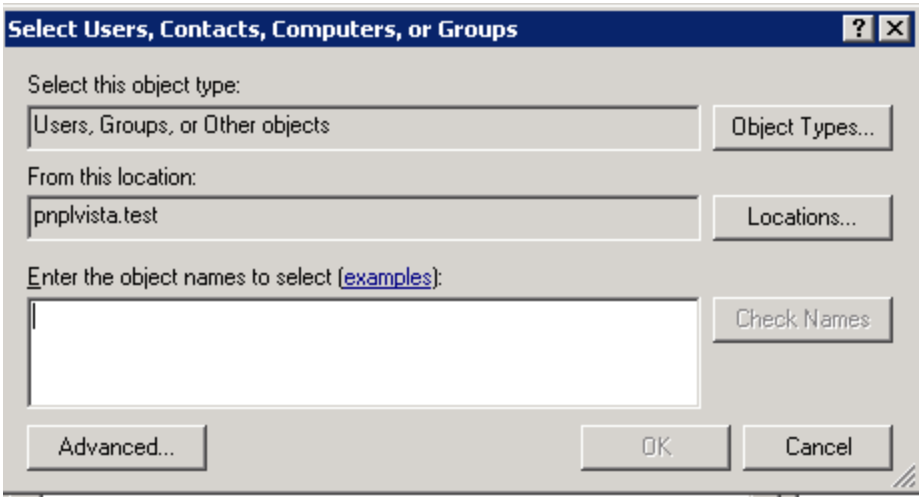


Figure 48

4. Type the user name in the **Enter the object names to select** field.

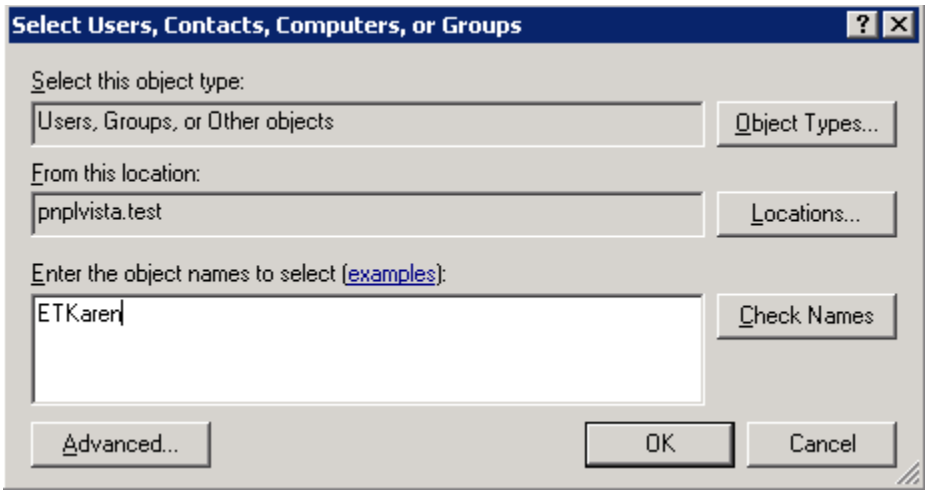


Figure 49

5. Select the **Check Names** button.

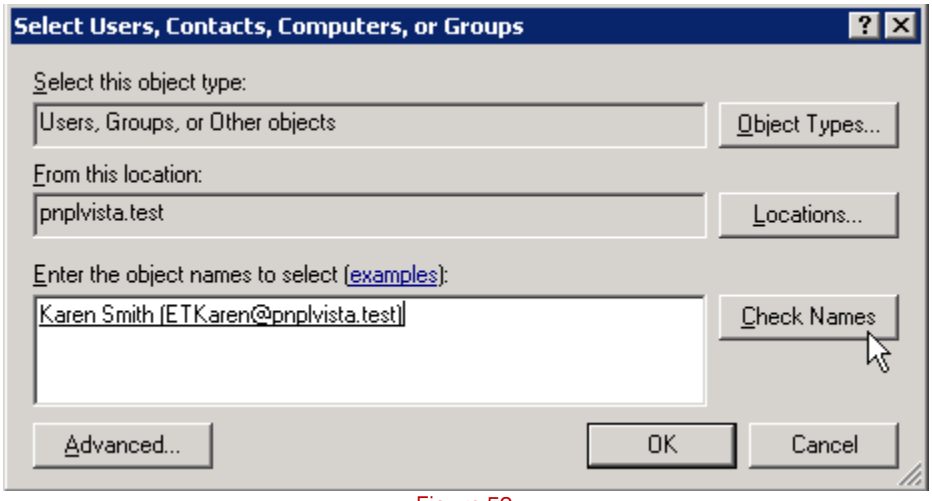


Figure 50

6. Select the **OK** button.

   'Karen Smith' is a member of 'EventTracker Test' group.

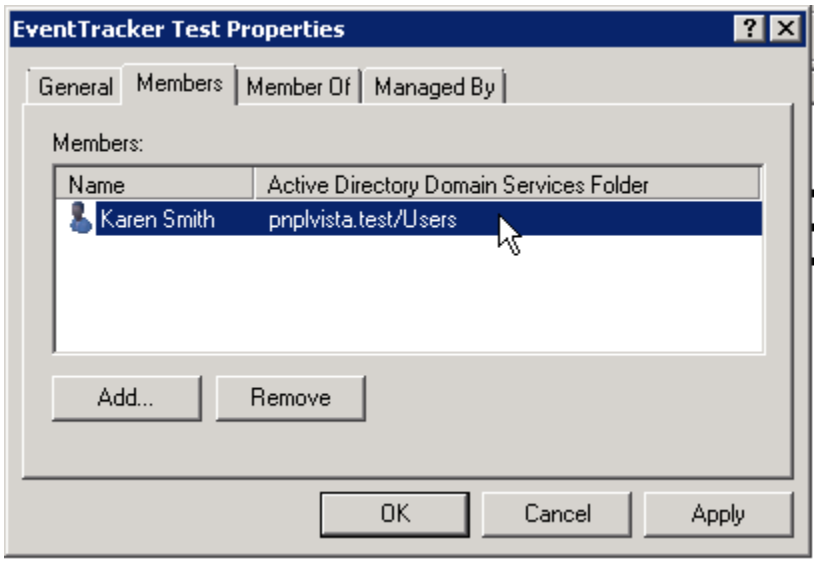


Figure 51

7. Select **Apply**, and then select the **OK** button.

Add User to Local Administrators group

To add a user in 'Administrators' group on the computer where EventTracker Enterprise is installed please follow the steps given below.

1) Right click **My Computer**, select **Manage**.
2) Expand **Local Users and Groups**, select **Groups.**
3) Right click **EventTracker** group, select **Add to Group**.

   EventTracker Properties window displays.
4) Select the **Add** button.

   Select Users, Contacts, Computers, Service Accounts, or Groups window displays.

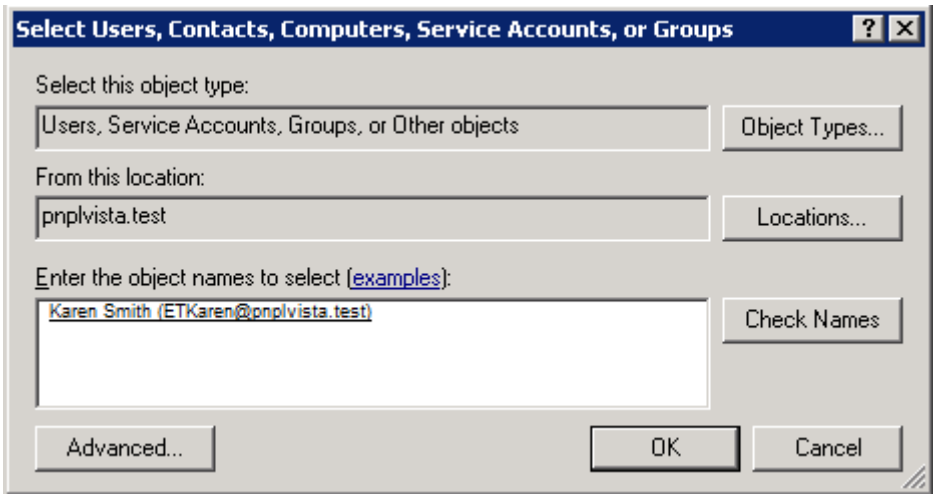


Figure 52

5) In **Enter the object names to select** box, enter username (i.e. 'Karen' in our example), and select the **Check Names** button.
6) Select the **OK** button.

Add cross-domain users

Consider Domain A and Domain B exist in Forest 1 and EventTracker Enterprise server is a member of Domain A. If a user in Domain B needs to access and administer EventTracker Enterprise, add that user to EventTracker user group in Domain A. Since these two domains exist in the same forest, Windows creates automatic trust relationship between these two domains.

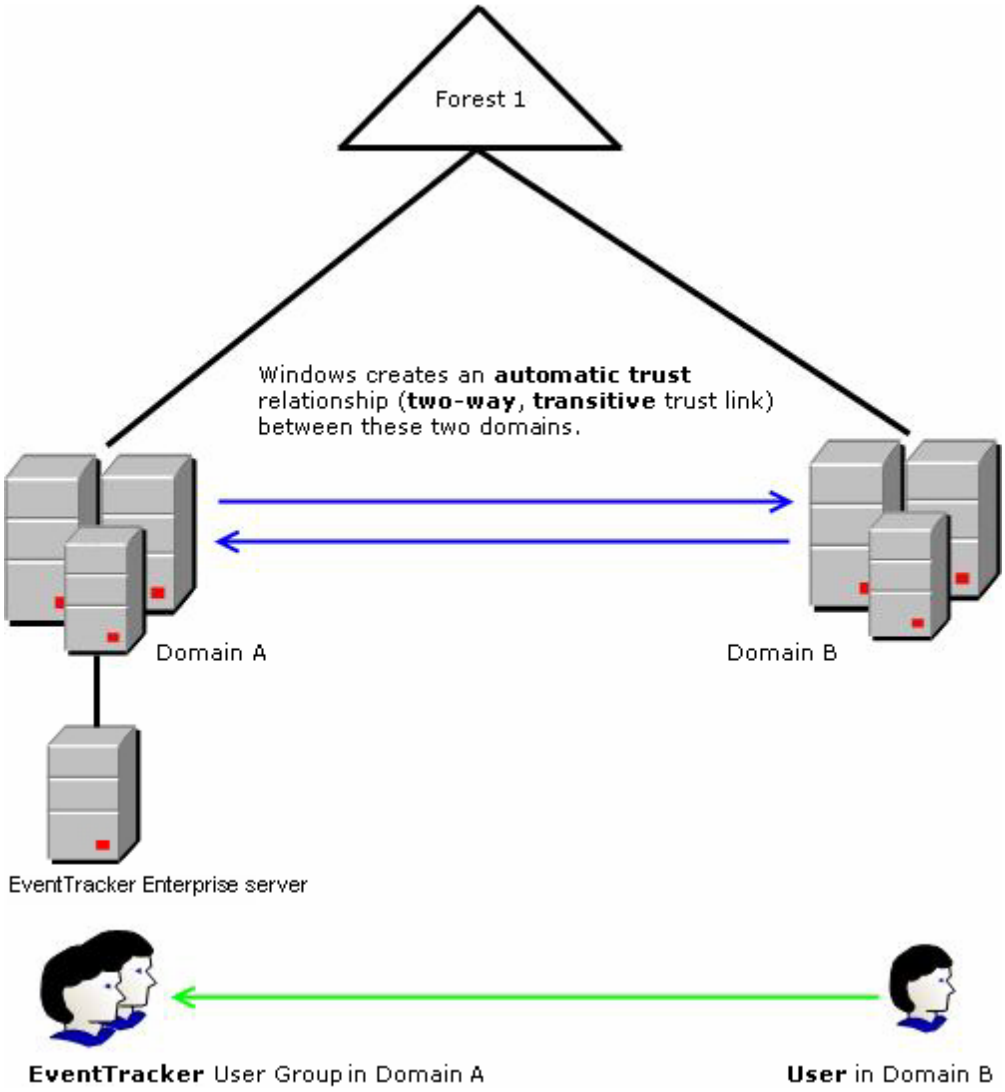

Forest 1
Windows creates an automatic trust relationship (two-way, transitive trust link) between these two domains.
Domain A
Domain B
EventTracker Enterprise server
EventTracker User Group in Domain A
User in Domain B

Figure 53

Add cross-forest users

Consider Domain A and Domain B exist in Forest 1 and Domain C and Domain D exists in Forest 2. EventTracker Enterprise server is a member of Domain A. If a user in Domain C needs to access and administer EventTracker Enterprise, add that user to EventTracker user group in Domain A. Since these two domains exist in different forests, you need to create trust prior to adding users.

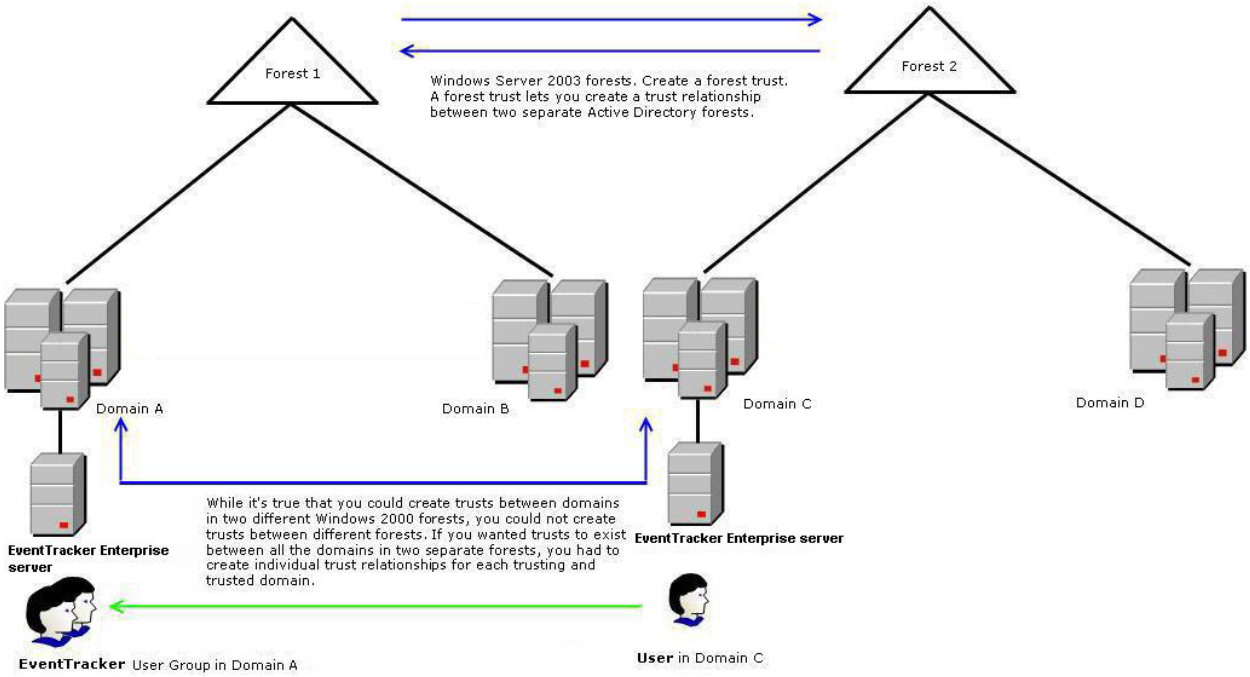

Forest 1
Forest 2
Windows Server 2003 forests. Create a forest trust.
A forest trust lets you create a trust relationship
between two separate Active Directory forests.
Domain A
Domain B
Domain C
Domain D
While it's true that you could create trusts between domains in two different Windows 2000 forests, you could not create trusts between different forests. If you wanted trusts to exist between all the domains in two separate forests, you had to create individual trust relationships for each trusting and trusted domain.
EventTracker Enterprise server
EventTracker Enterprise server
EventTracker User Group in Domain A
User in Domain C

Figure 54

Windows Server 2003 forests: Create a forest trust. A forest trust lets you create a trust relationship between two separate Active Directory forests.

Install EventTracker Manager

Prism recommends you to refer "EventTracker Architecture" guide before you begin installation. This guide explains the architecture and sample deployment methods with illustrations.

Installation can be initiated by the following methods.

1. Launch the executable program. The installation is geared to be intuitive and friendly. During install you will be asked to provide the path of the digital certificate. Certificate is validated against the latest CRL. Installation proceeds further only if the Certificate found to be valid.

   The installation procedure is identical for all operating system(s) as mentioned in Table 3.

Pre-install Checklist for EventTracker Manager

The pre-install checklist describes the specific settings, permissions, and privileges that are required for installing EventTracker Manager. Read the checklist before installation to avoid installation failure.

ENSURE	**User is a member of 'Local Administrators' group**
	MSI package installation is allowed
	User has 'Logon As Service' rights
	User has 'Logon As Batch job' rights
	Network Discovery is enabled
	System cryptography: Use FIPS 140 compliant cryptographic algorithms, with encryption, hashing and signing algorithms disabled.
VERIFY	User has permission on 'Application install directory' (Folders and sub folders).
	User must have create service permission on the target system(SCM- service control manager)
	User has Read/Write permission on windows registry.

Table 5

IIS Settings

Please ensure that IIS Settings under Application Pools are as follows in Windows 2008/2008 R2/2012/2012 R2.

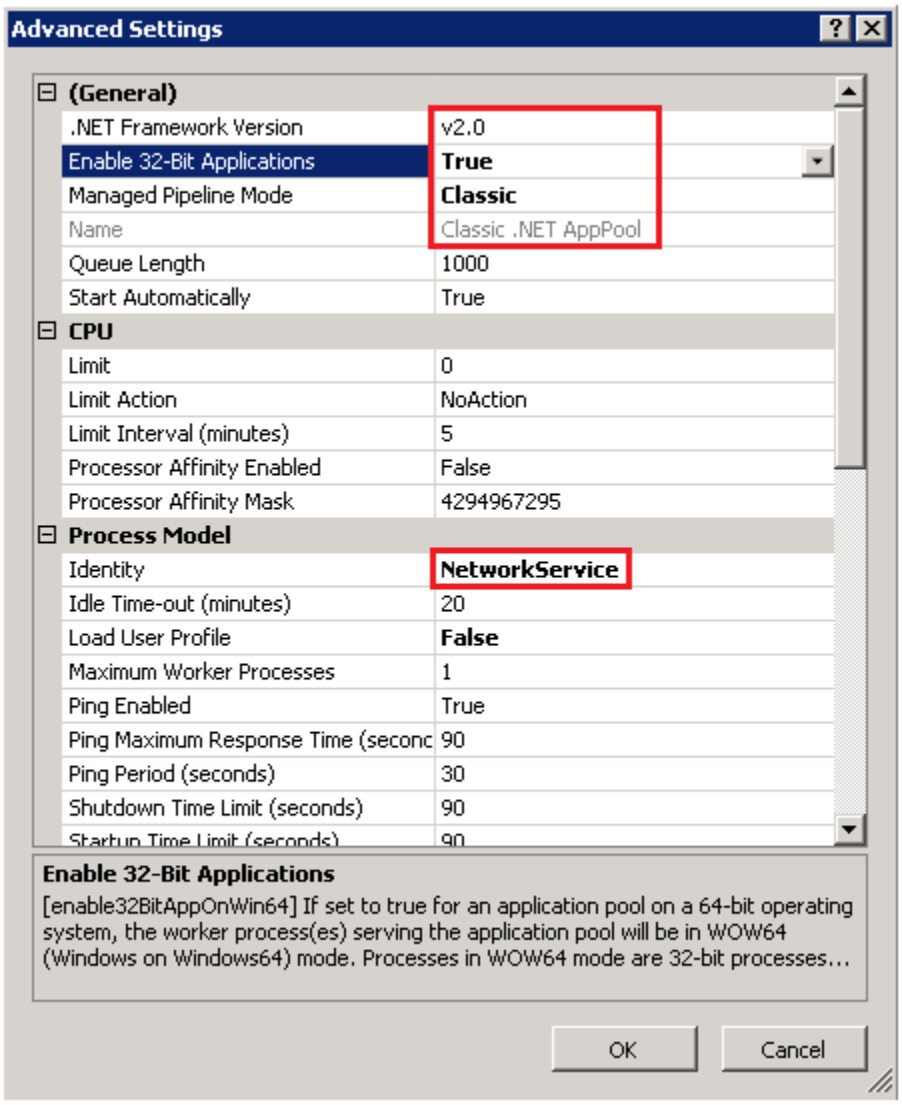


Figure 55 – 64 bit OS

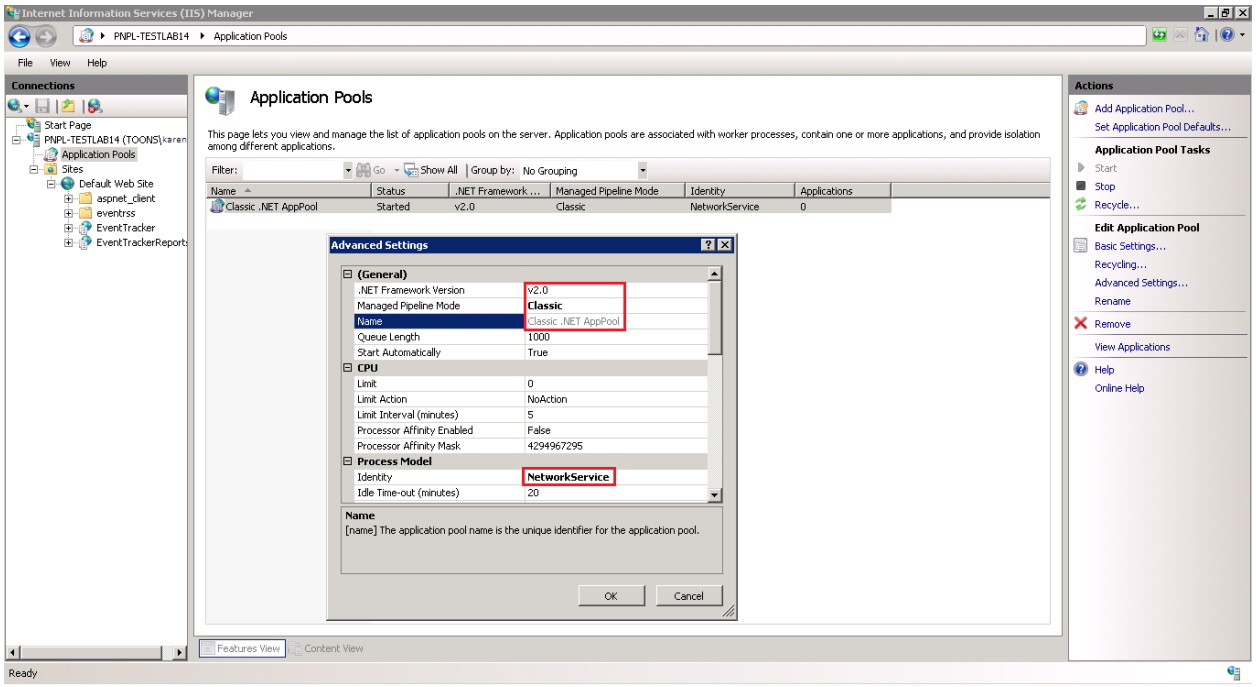


Figure 56 – 32 bit OS

For details to configure the above settings, please refer Install and Customize IIS Web Server Guide.

Procedure to install EventTracker Manager v7.5.53 - Custom

If you are using EventTracker for the first time, launch the executable program and proceed. If you are a second time user, please uninstall the previous version of EventTracker and then proceed. The detail procedure to uninstall EventTracker is mentioned in Uninstall EventTracker.

The detail procedure to install EventTracker is given below.

1. Double-click the executable file.

   EventTracker Pre-Install Check window displays.

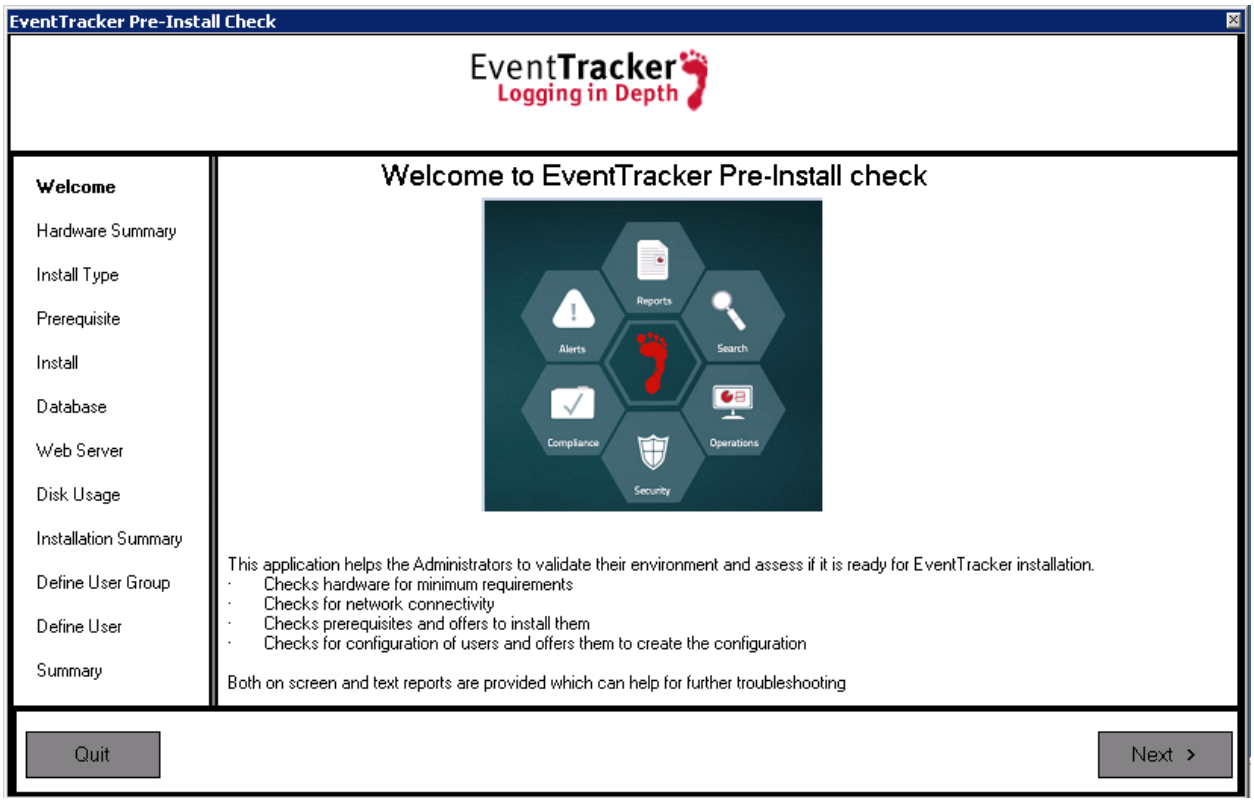


Figure 57

2. Click the **Next >** button.

   Hardware Summary pane displays.

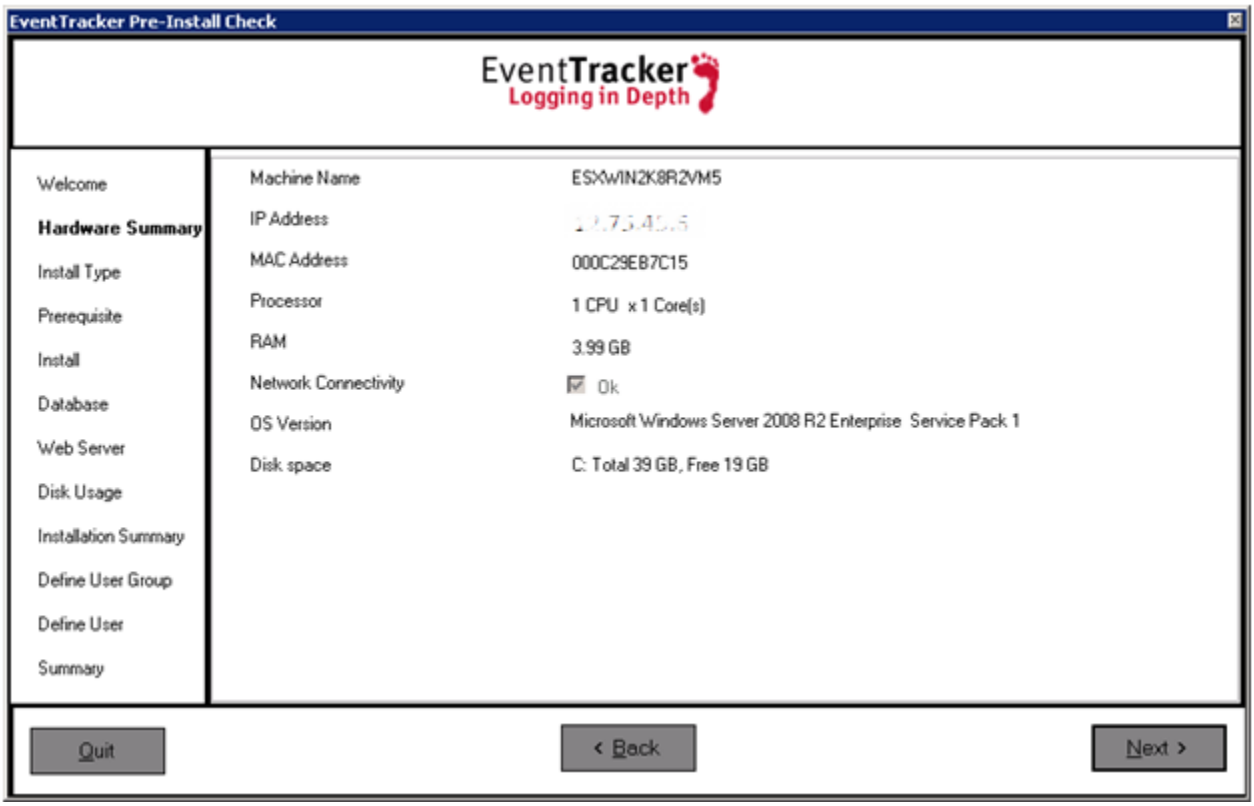


Figure 58

3. Click the **Next >** button.

   Install Type page displays.

4. Select **Standard/Collection Point/Custom** option, and then select the **Next >** button.

   In this section, Custom option is selected.

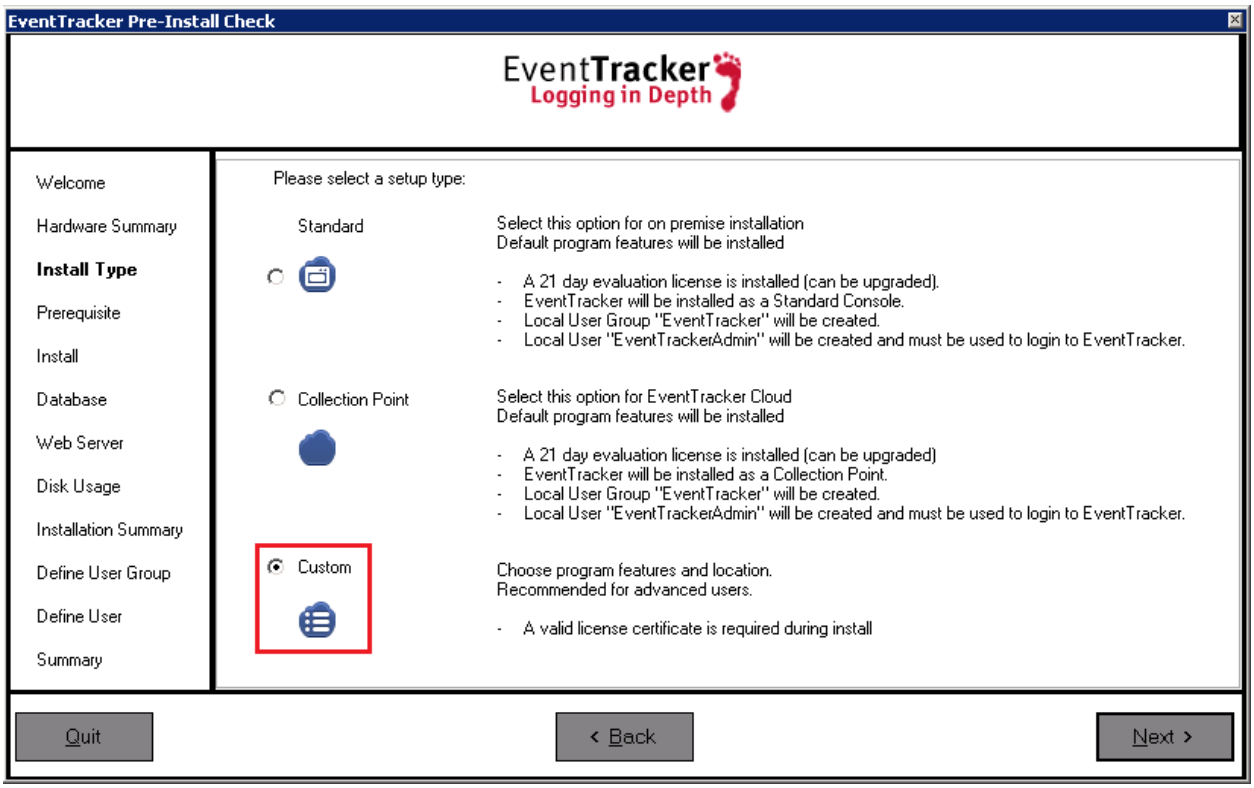

EventTracker Pre-Install Check
EventTracker
Logging in Depth
Welcome
Hardware Summary
Install Type
Prerequisite
Install
Database
Web Server
Disk Usage
Installation Summary
Define User Group
Define User
Summary
Please select a setup type:
Standard
Select this option for on premise installation
Default program features will be installed
- A 21 day evaluation license is installed (can be upgraded).
- EventTracker will be installed as a Standard Console.
- Local User Group "EventTracker" will be created.
- Local User "EventTrackerAdmin" will be created and must be used to login to EventTracker.
Collection Point
Select this option for EventTracker Cloud
Default program features will be installed
- A 21 day evaluation license is installed (can be upgraded)
- EventTracker will be installed as a Collection Point.
- Local User Group "EventTracker" will be created.
- Local User "EventTrackerAdmin" will be created and must be used to login to EventTracker.
Custom
Choose program features and location.
Recommended for advanced users.
- A valid license certificate is required during install
Quit
< Back
Next >

Figure 59

Prerequisite page displays.

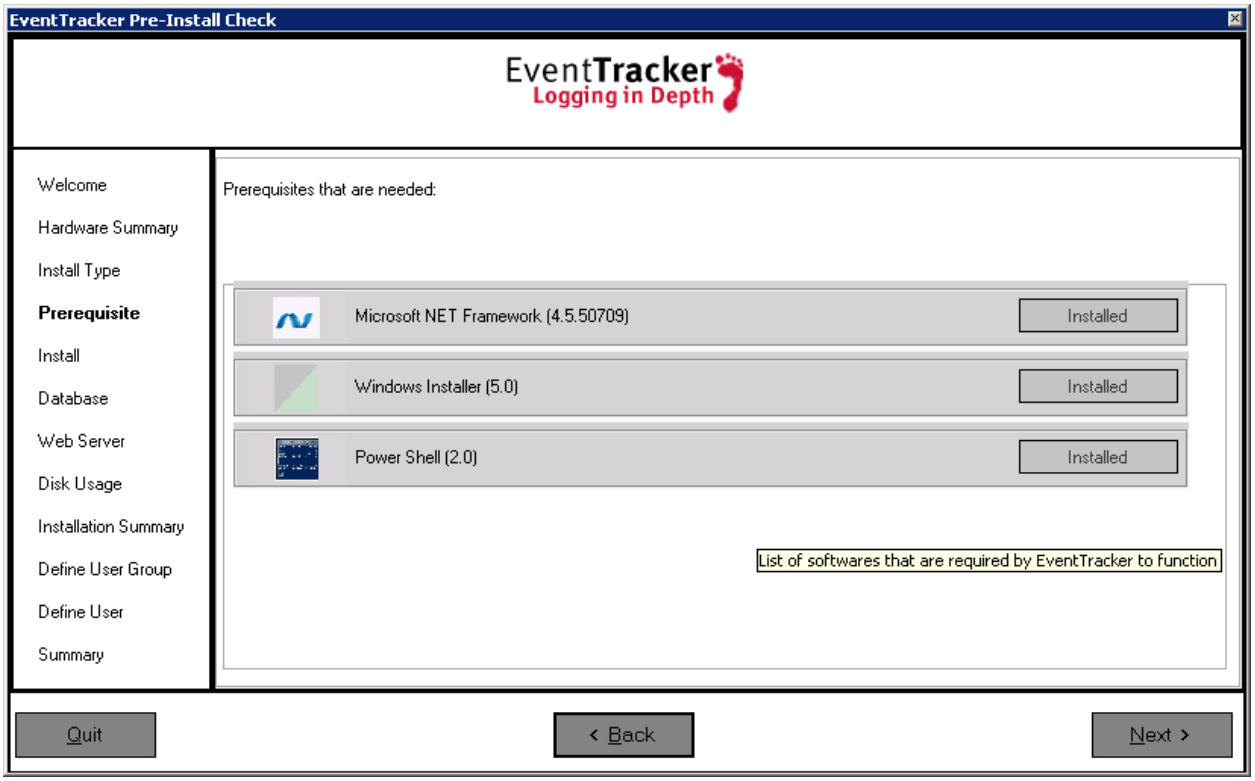


Figure 60

NOTE:

- If the prerequisites are not installed, then a message 'To be installed' displays against the respective prerequisite.

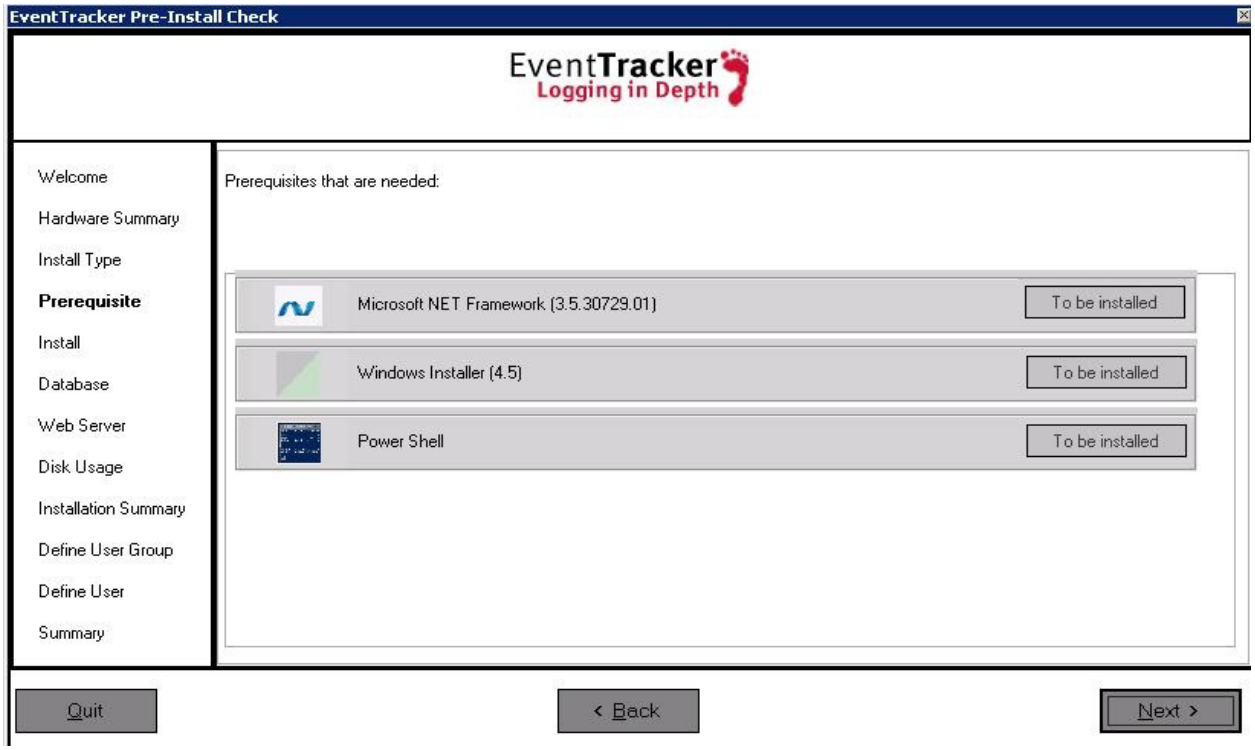


Figure 61

a. Click the **Next >** button.

   Install page displays.

- For some Windows platforms, .NET Framework has to be installed via Server Manager.

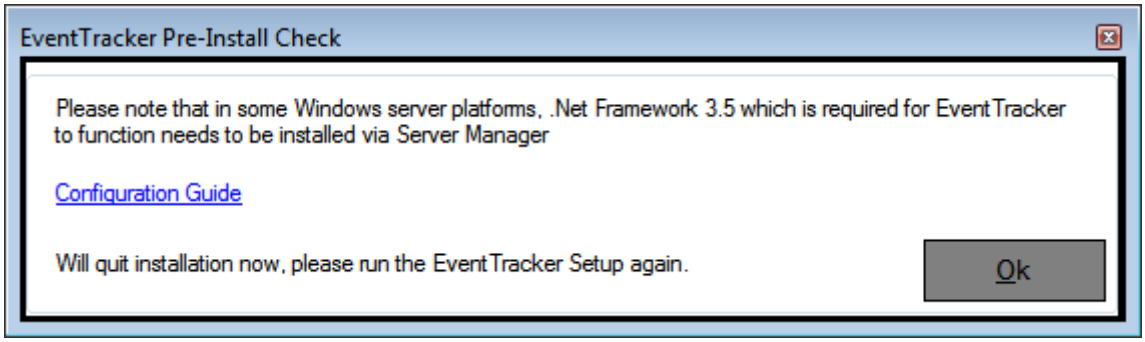

EventTracker Pre-Install Check
Please note that in some Windows server platforms, .Net Framework 3.5 which is required for EventTracker to function needs to be installed via Server Manager
Configuration Guide
Will quit installation now, please run the EventTracker Setup again.
Ok

Figure 62

- Click **Configuration Guide** link for detail instructions to configure .NET Framework.

  The instructions to install .NET Framework is given in detail in How To - Install Microsoft .NET Framework.

- Click **OK** and proceed to install .NET Framework.

- After successfully installing .NET Framework, rerun the executable file once again.

(OR)

- If Microsoft .NET Framework is not installed, click **Next >**, and then click the **Install** button.

  Please refer Figure 63.

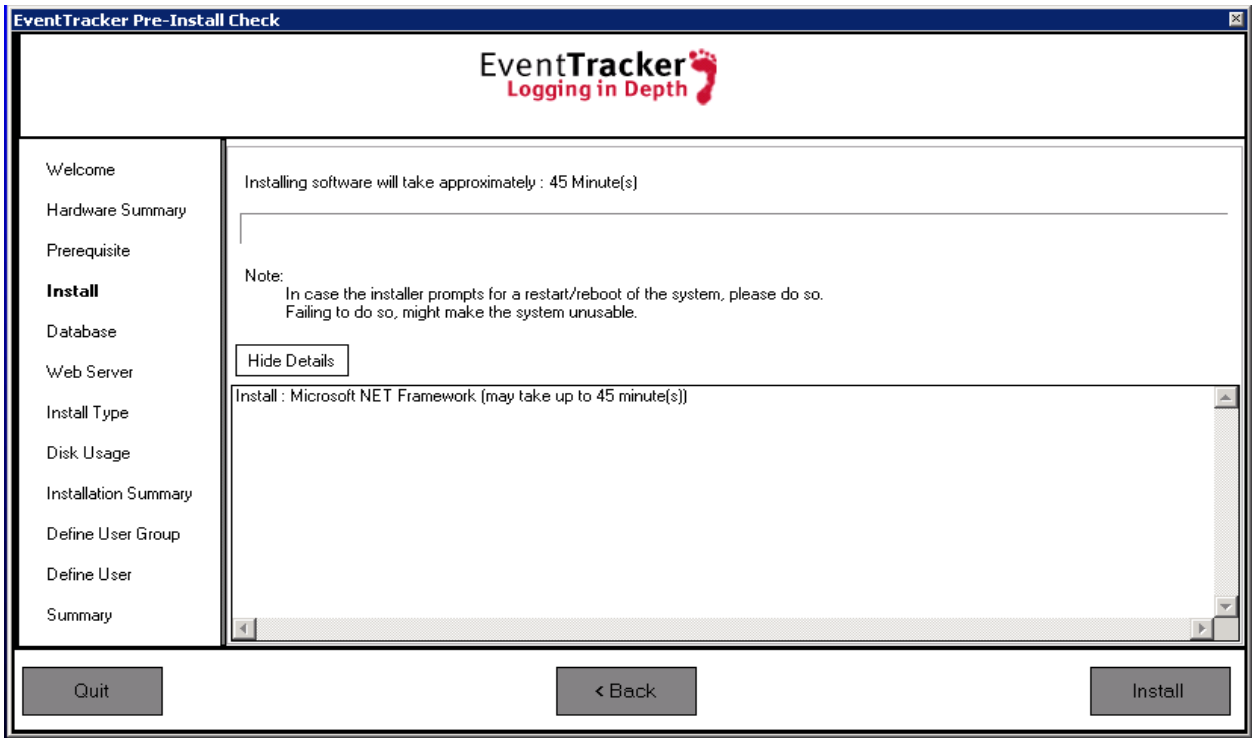


Figure 63 – Installing Microsoft .NET Framework

- If Windows Installer, Power Shell is not installed, click **Next >** and then click the **Install** button.

  Please refer Figure 64 respectively.

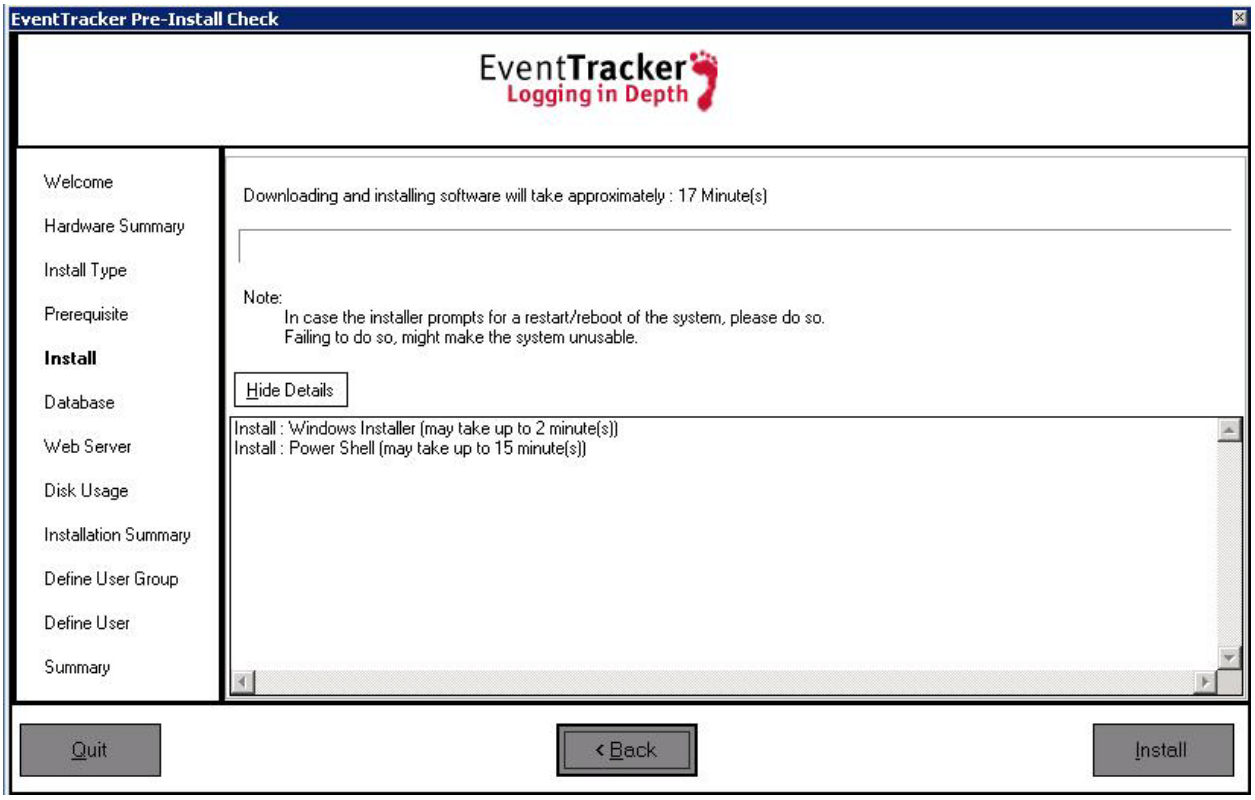


Figure 64 – Installing Windows Installer and Powershell

Once prerequisites are installed, Database page displays.

5. If **MSSQL Server – Express Edition 2005/2008/2008 R2/2012** is already installed, then click the **Next >** button.

NOTE:

Users are allowed to choose any version of MS SQL required. On OS greater than Vista, SQL 2008 R2 Express is installed. On Vista and below, SQL 2005 Express is installed.

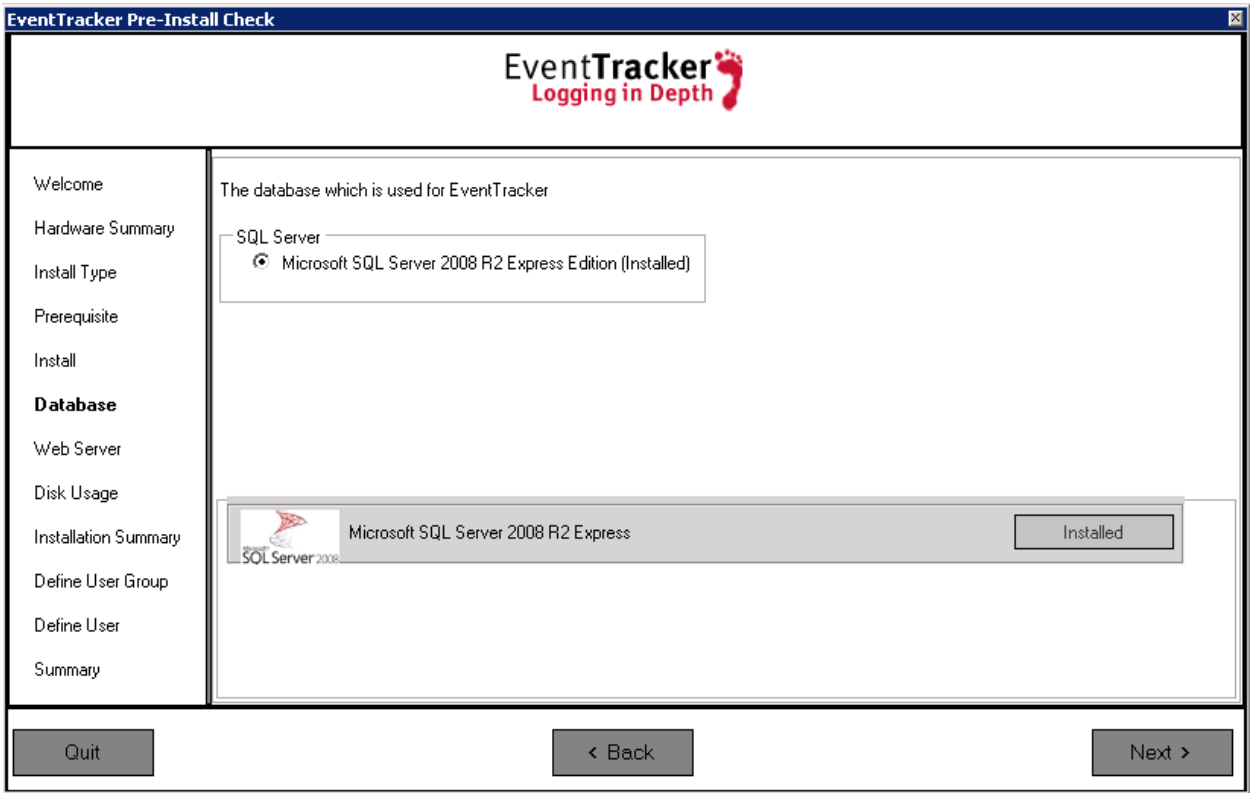


Figure 65

Web Server page displays.

- If MS SQL Express is not installed, then click **Next >**.

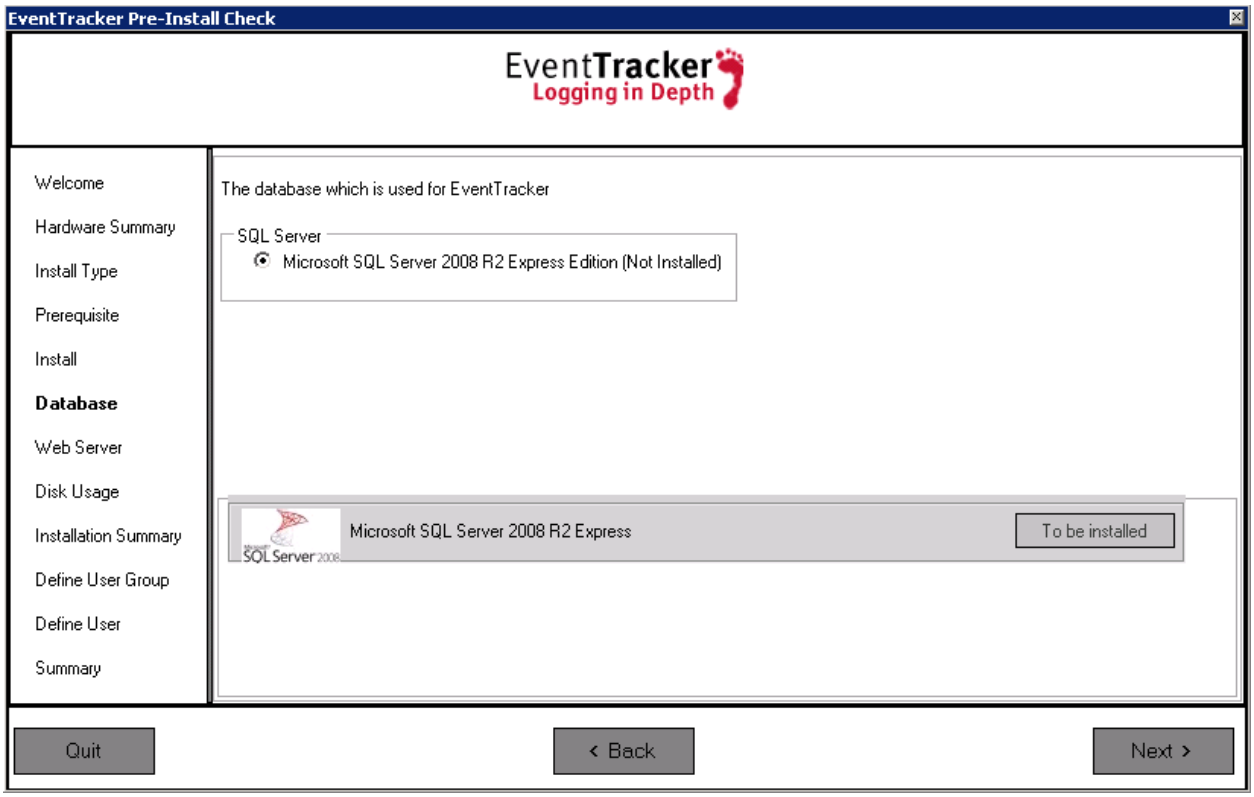


Figure 66

The pre-installer prompts to download SQL Server Express Edition.

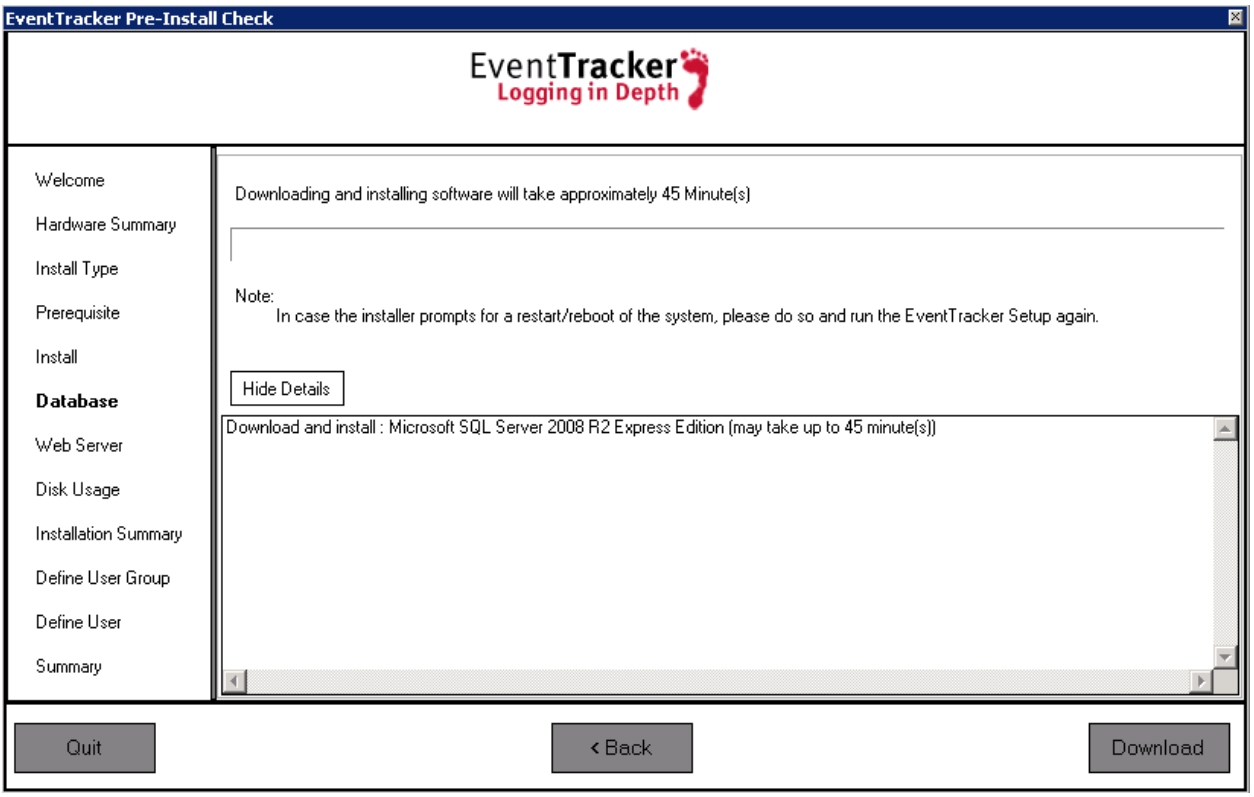


Figure 67

a. Click the **Download** button.

   Please select a location to download the SQL installer window displays.

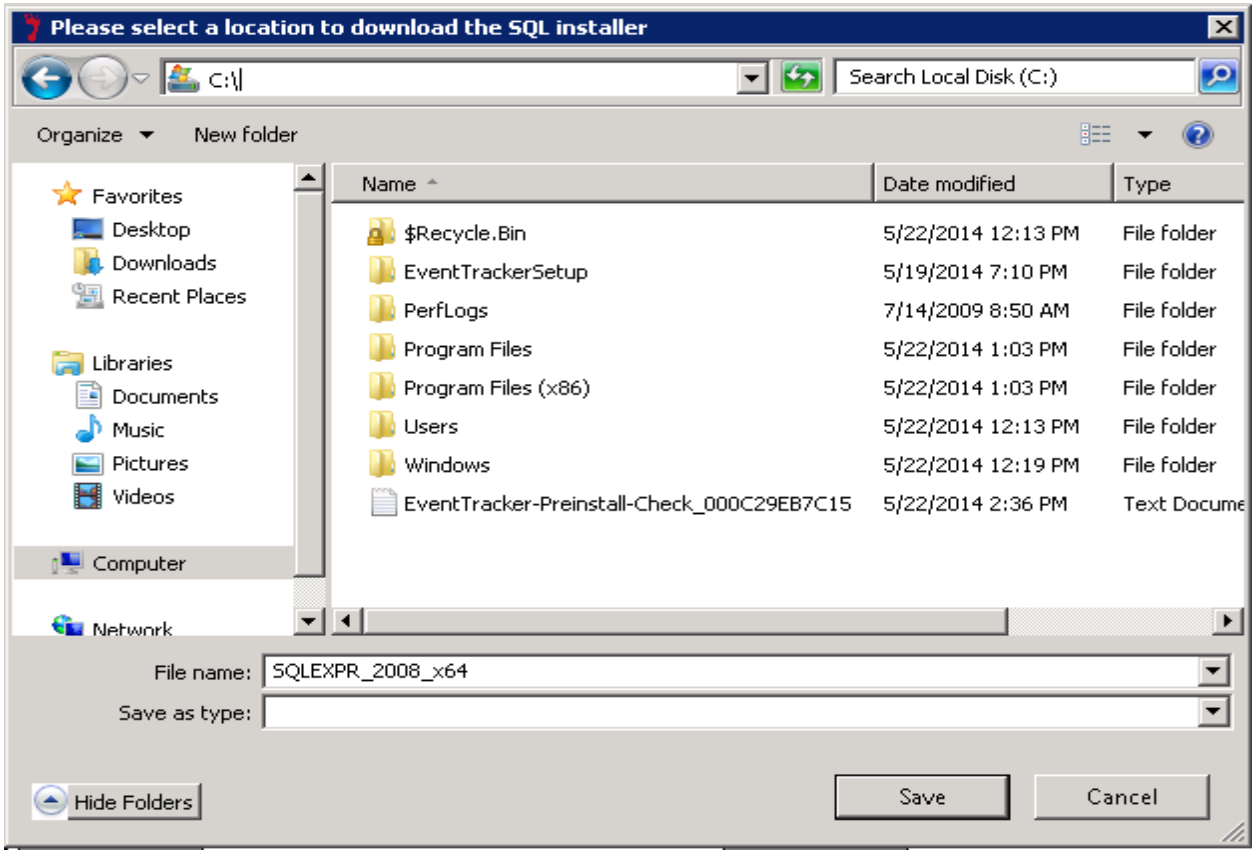


Figure 68

b. Select the path to download SQL Express on a particular location and then click **Save**.

SQL Express starts downloading and is installed in the background.

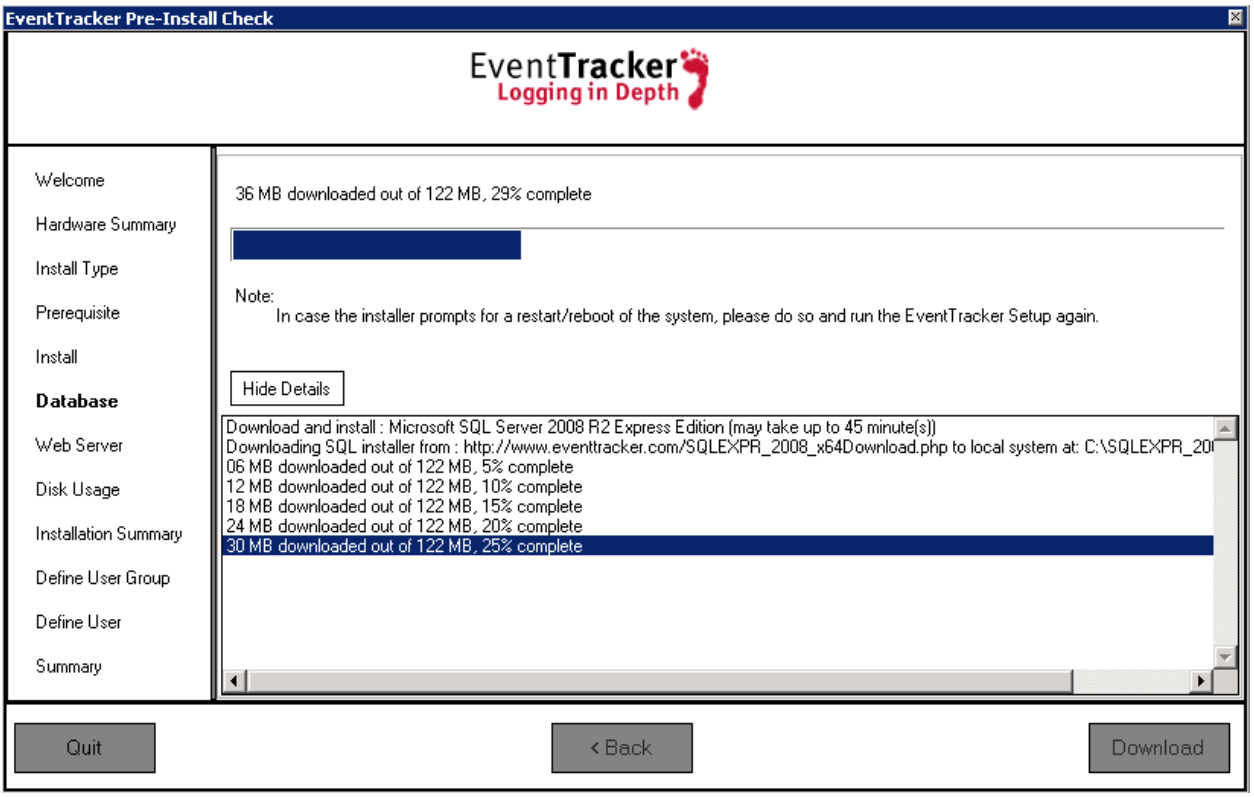

EventTracker Pre-Install Check
EventTracker
Logging in Depth
Welcome
Hardware Summary
Install Type
Prerequisite
Install
Database
Web Server
Disk Usage
Installation Summary
Define User Group
Define User
Summary
36 MB downloaded out of 122 MB, 29% complete
Note:
In case the installer prompts for a restart/reboot of the system, please do so and run the EventTracker Setup again.
Hide Details
Download and install : Microsoft SQL Server 2008 R2 Express Edition (may take up to 45 minute(s))
Downloading SQL installer from : http://www.eventtracker.com/SQLEXPR_2008_x64Download.php to local system at: C:\SQLEXPR_20
06 MB downloaded out of 122 MB, 5% complete
12 MB downloaded out of 122 MB, 10% complete
18 MB downloaded out of 122 MB, 15% complete
24 MB downloaded out of 122 MB, 20% complete
30 MB downloaded out of 122 MB, 25% complete
Quit
< Back
Download

Figure 69

After MS SQL Express is installed, Web Server page displays.

6. Select **IIS Express** option, and then select the **Next >** button.

NOTE:

- Only IIS Express will be installed, if IIS is not installed on the machine.
- From now on we are supporting IIS Express since it is a lightweight tool. You can choose to install IIS Express/Manager based on the requirement.
- If you prefer to use IIS Manager, click **Configuration Guide** link for detail instructions to install IIS.

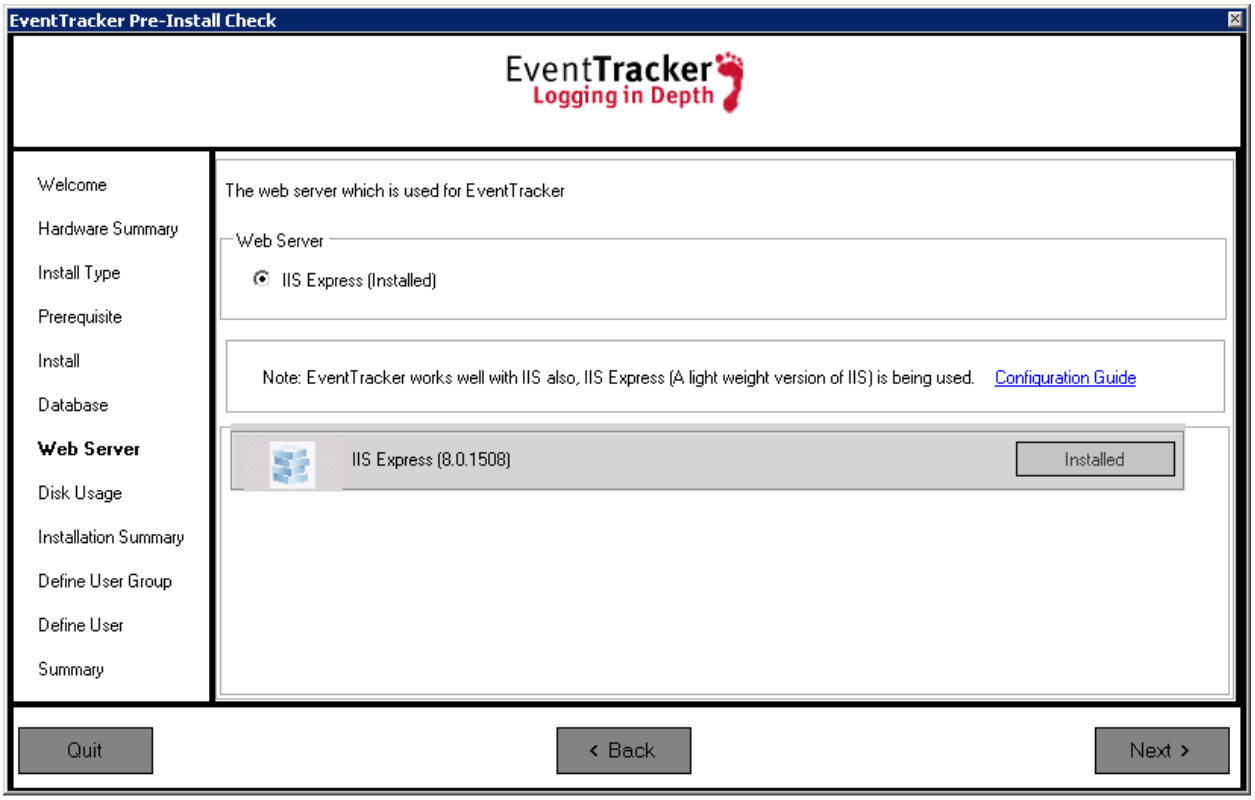


Figure 70

If IIS Express is already installed, on clicking **Next >, Disk Usage** page displays.

If IIS Express is not installed, please refer Figure 71 and proceed to install it.

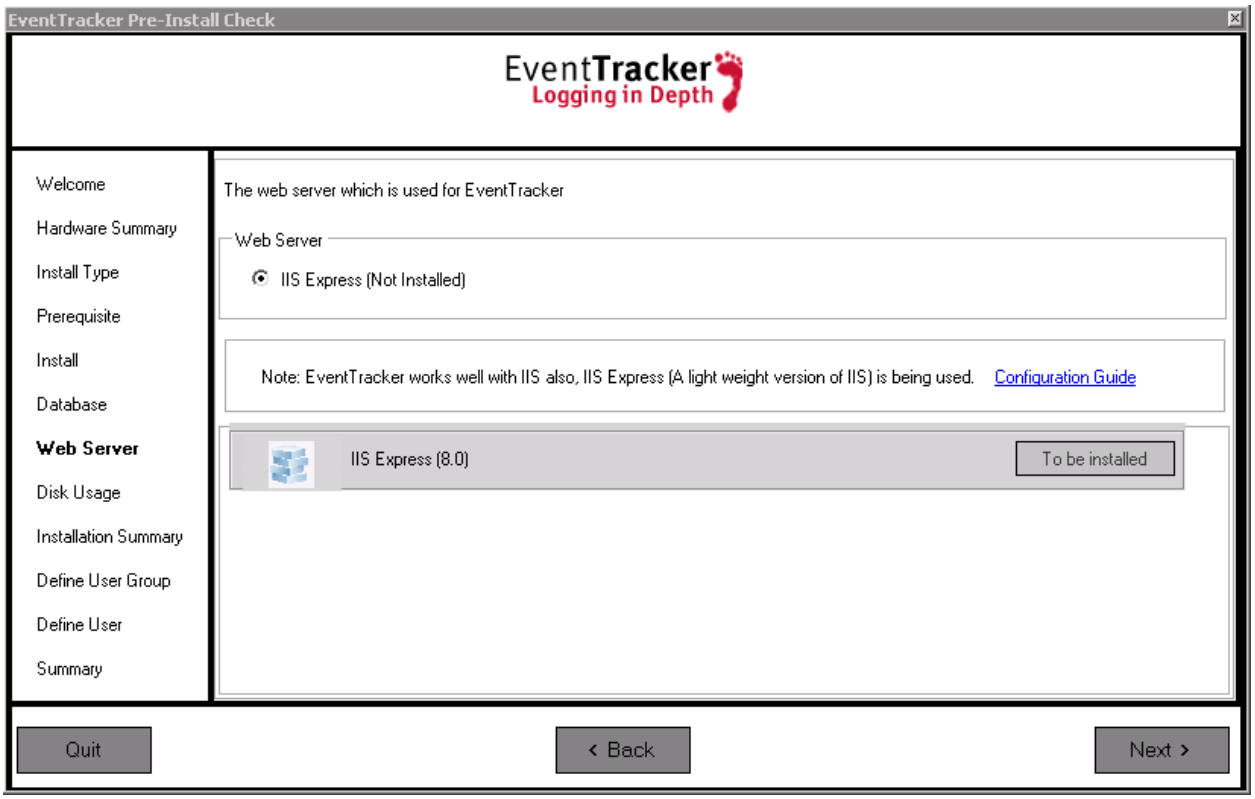


Figure 71

a. If **IIS Express (Not Installed)** option is selected, then click the **Next >** button.

Installation of IIS Express proceeds.

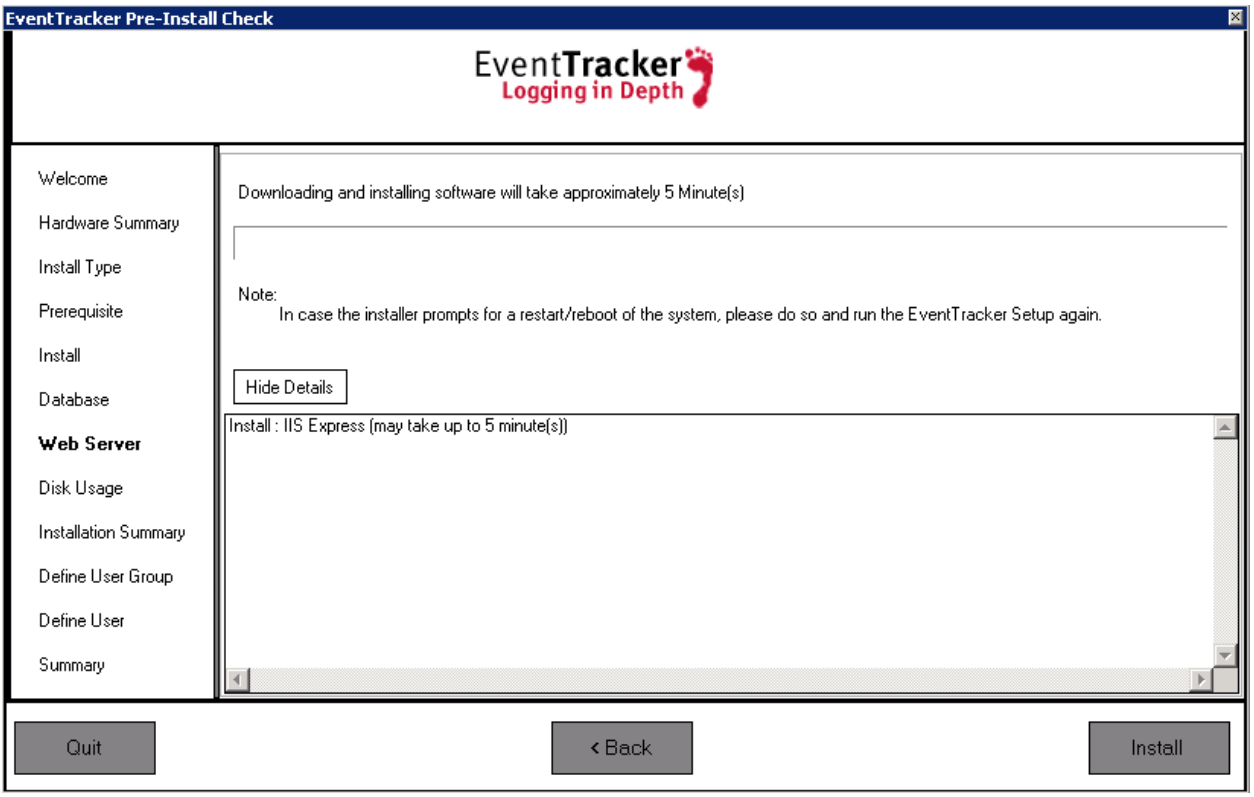


Figure 72

b. Click the **Install** button.

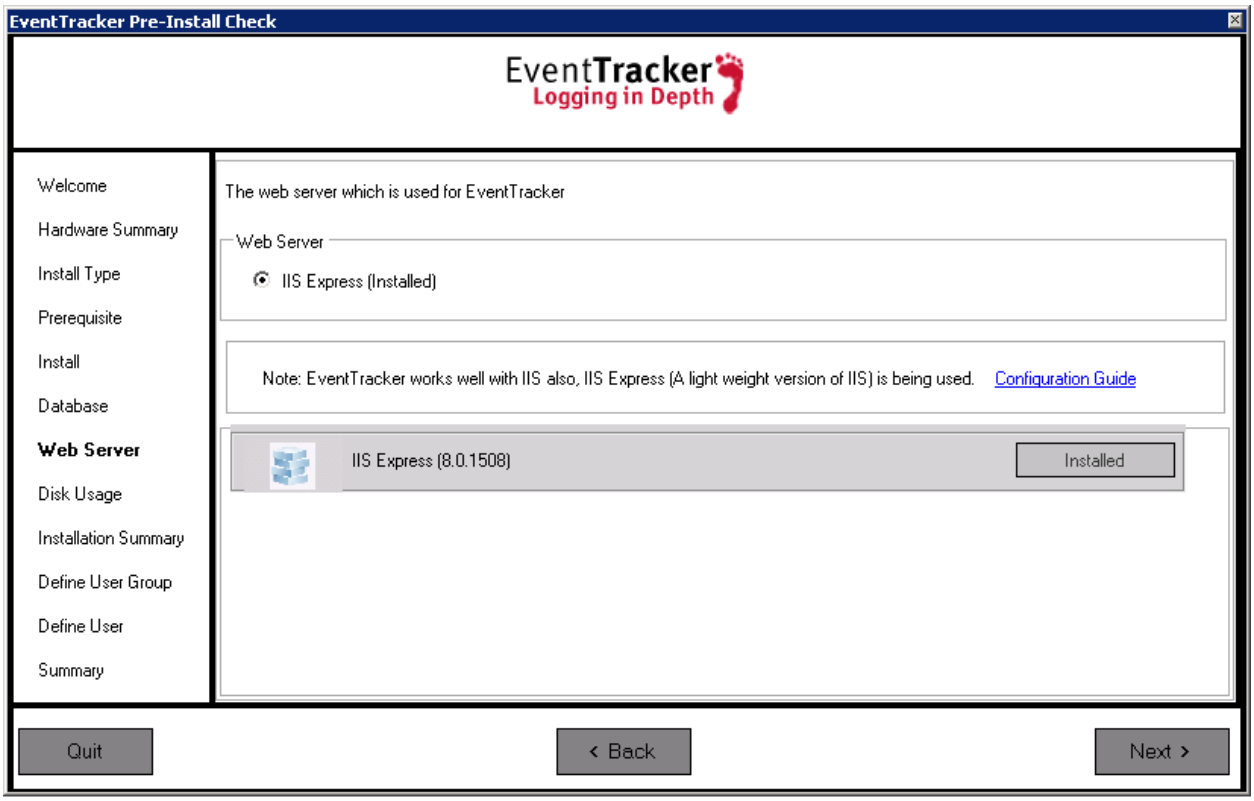


Figure 73

c. After IIS Express is installed successfully, click the **Next >** button.

Disk Usage page displays.

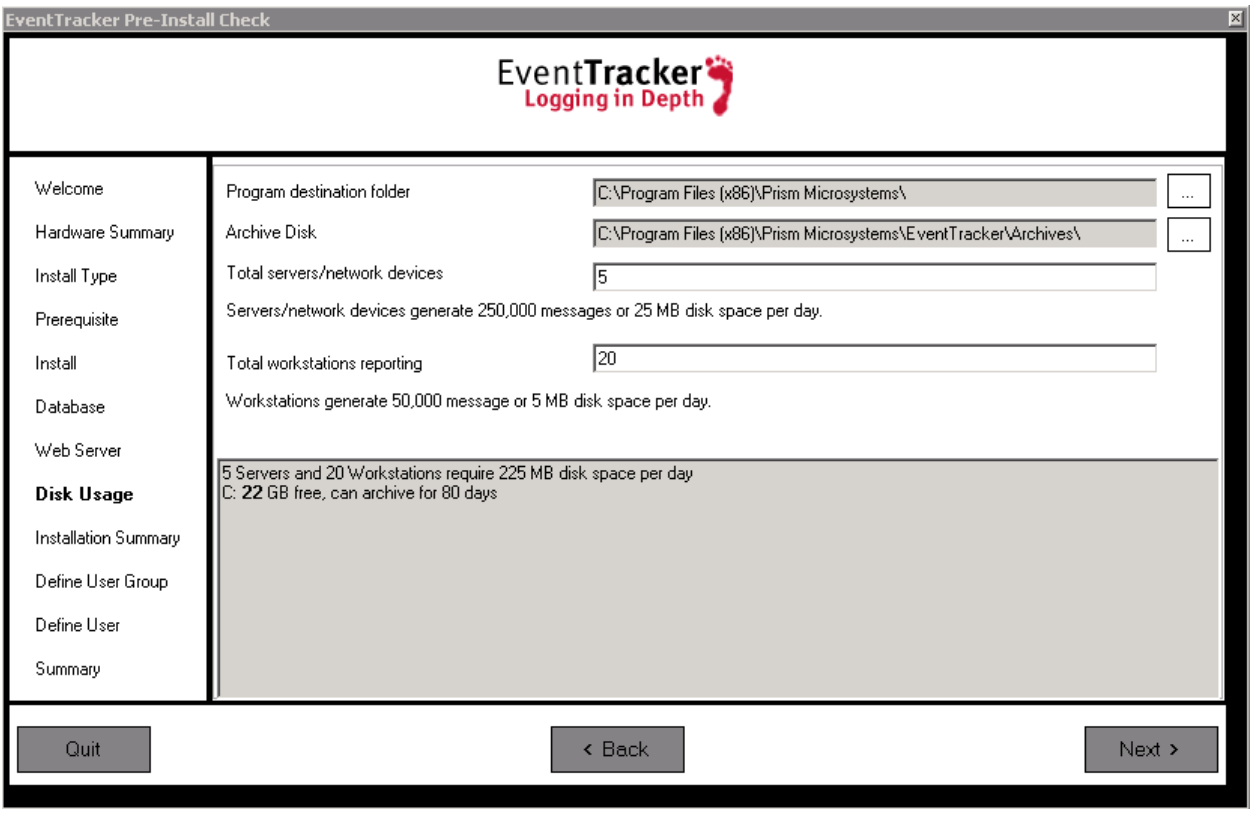


Figure 74

7. Click the **Next >** button.

   Installation Summary page displays.

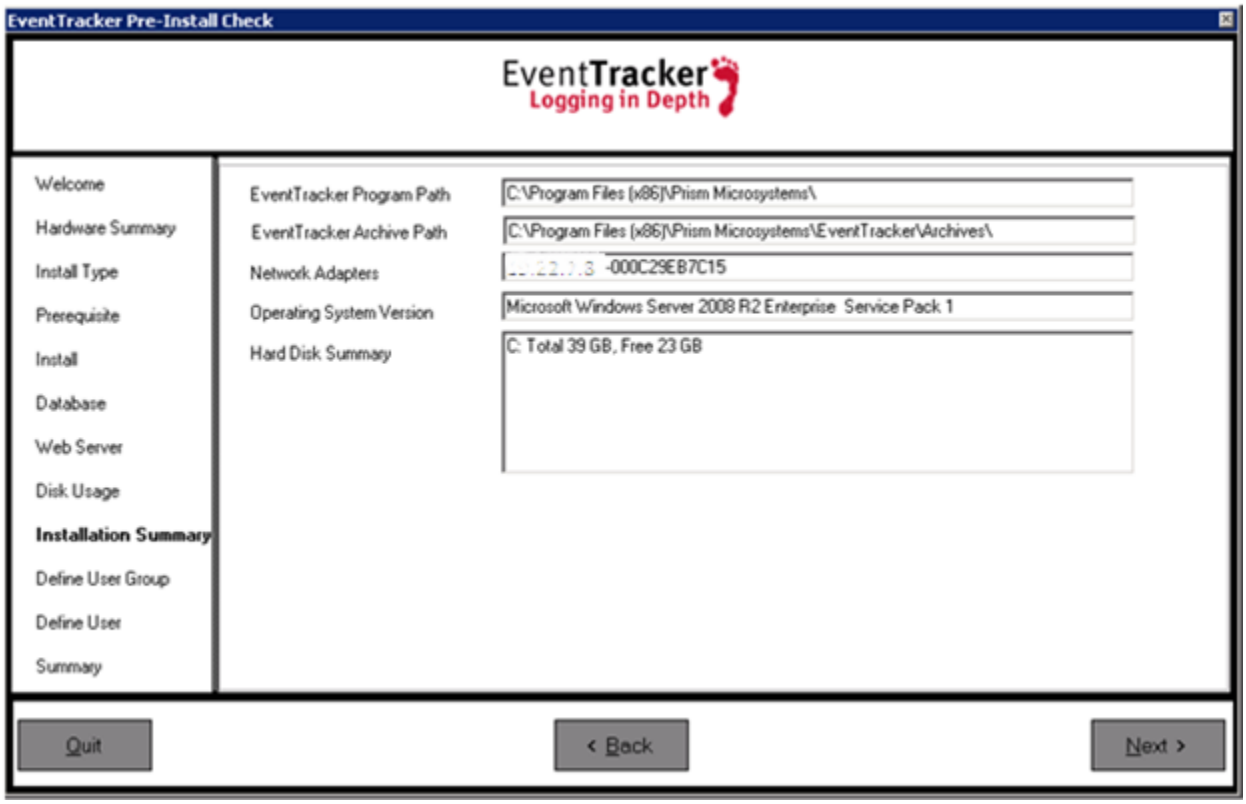


Figure 75

8. Click the **Next >** button.

   Define User Group page displays.

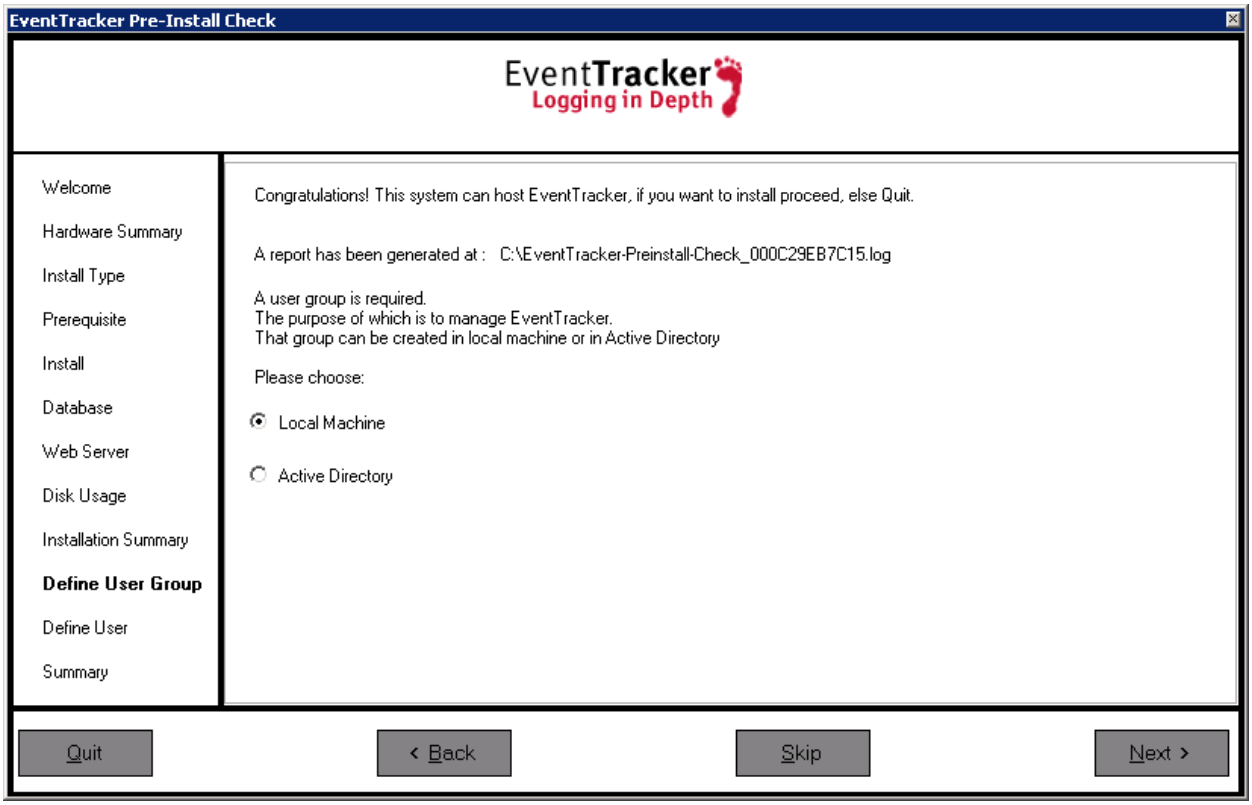


Figure 76

9. Select **Local Machine** or **Active Directory** option, and then select the **Next >** button.

   If **Local Machine** option is selected, then **You have selected to use local machine** page displays. Please refer step 10 for further instructions.

   NOTE:

   While creating group and/or user, the user should be part of the administrators group in the local machine. The user should have 'Logon as Batch' and 'Logon as Service' rights granted.

   If **Active Directory** option is selected, then **You have selected Active Directory domain:** page displays. Please refer Step 11 , for further instructions.

10. Select **Create User Group EventTracker** or **Select existing User Group** option, and then select the **Next >** button.

    If local machine was selected earlier, then '**You have selected to use local machine**' page displays.

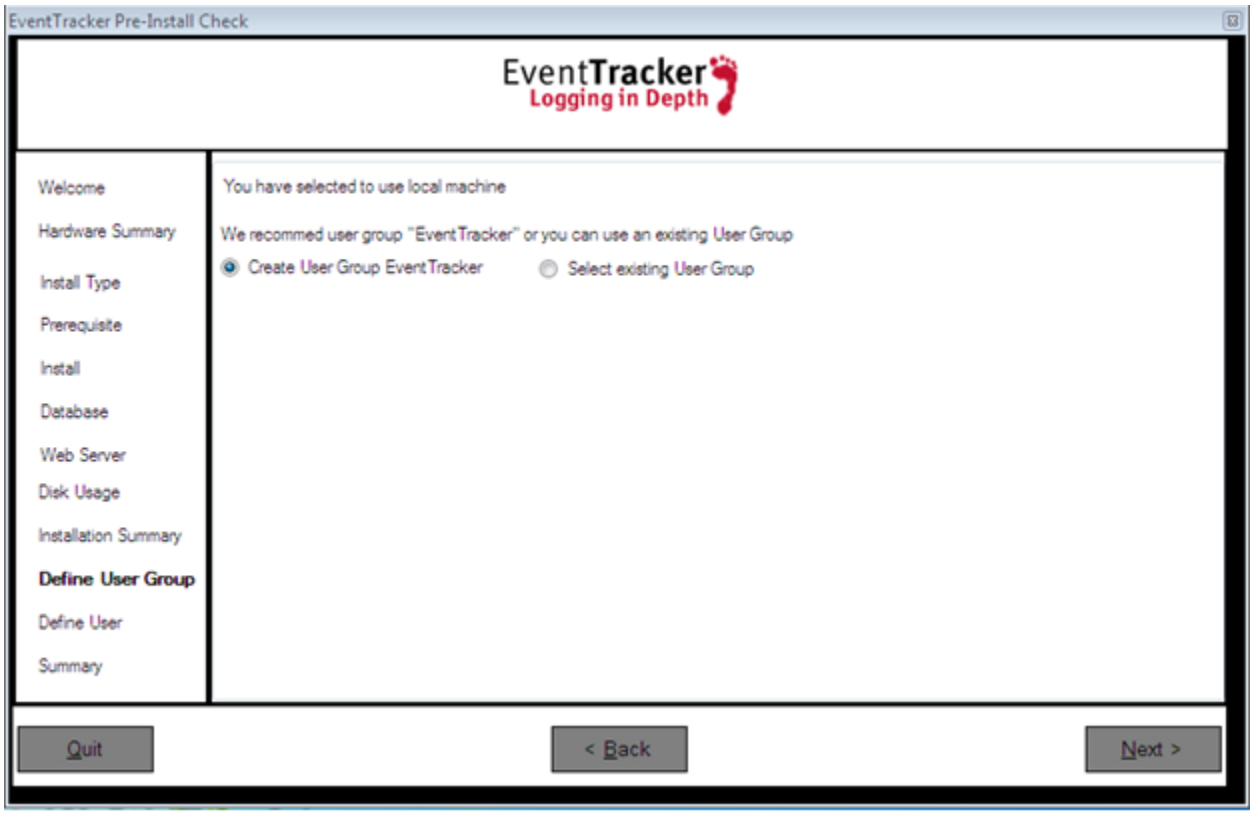


Figure 77

NOTE:

When creating group,

- We encourage users to use the group name as 'EventTracker', though EventTracker works with any group name.
- In case this group name does not exist then the default choice will be to 'Create User Group EventTracker' else the default choice will be 'Select Existing Group'.

a. If **Create User Group EventTracker** is selected, click **Next >**.

   Members of this User Group can access EventTracker page displays.

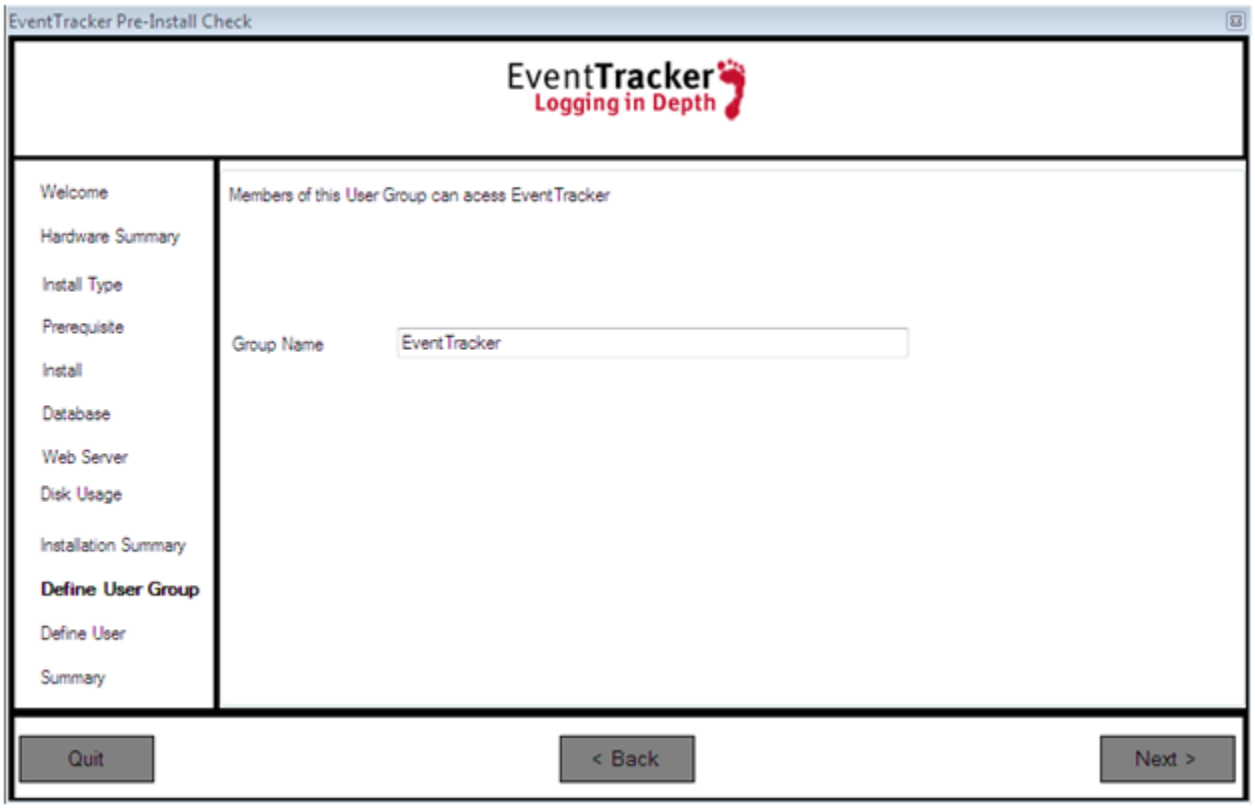


Figure 78

The group name must be unique otherwise an error message displays stating that the group already exists.

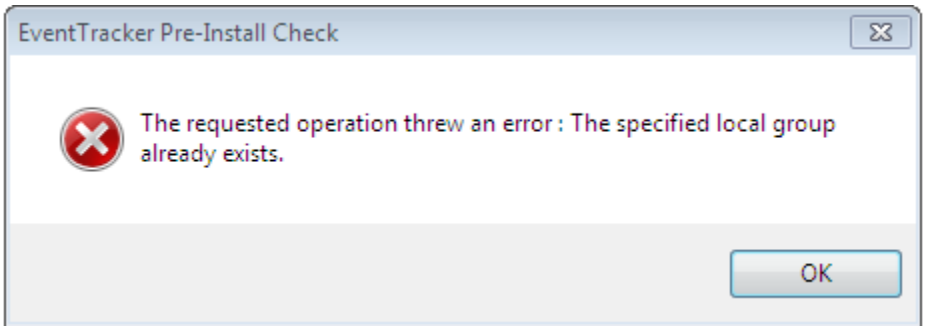


Figure 79

b. Click the **OK** button.

c. To solve this issue, enter a unique **Group Name**, and then click the **Next >** button.

Define User page displays. Please refer step 12 to continue installing EventTracker.

(OR)

a. If **Select existing User Group** option is selected, then select any group, and then click the **Next >** button.

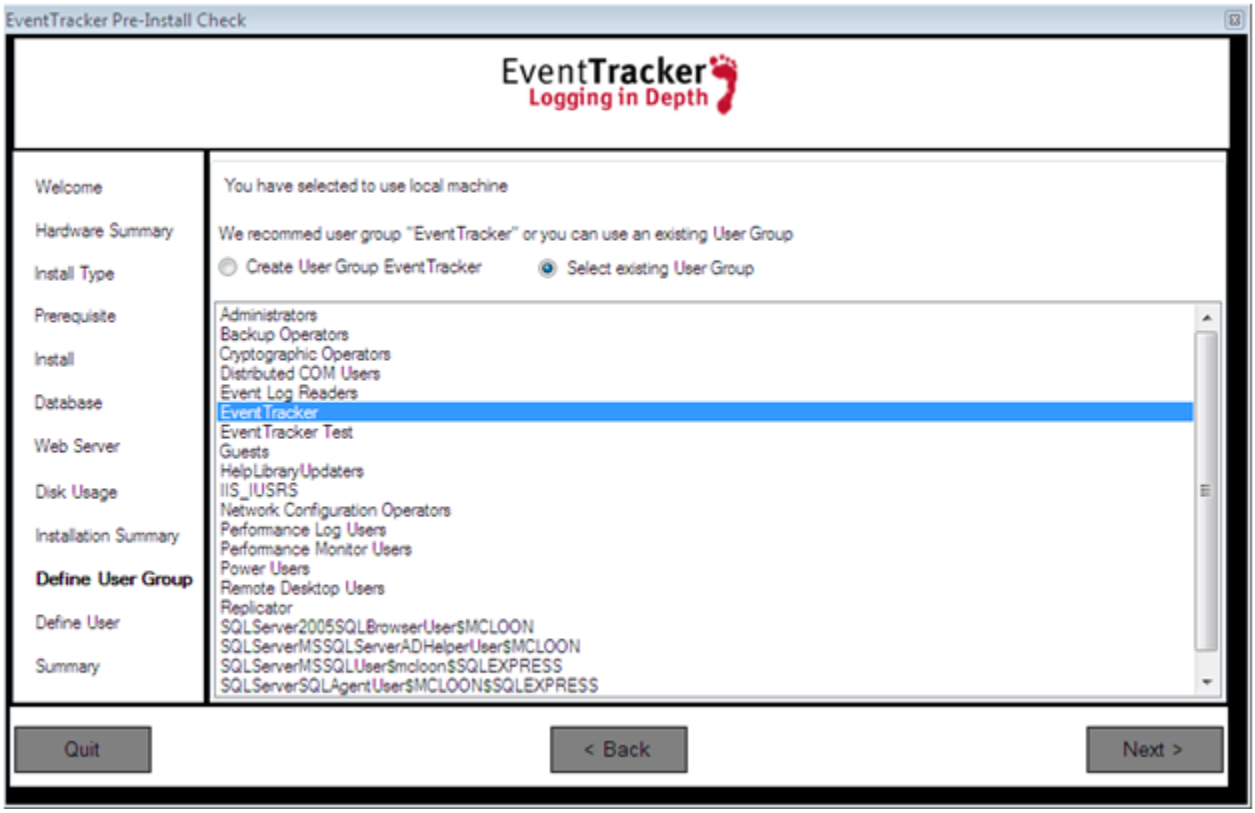


Figure 80

Define User page displays. Please refer step 12 to continue installing EventTracker.

If **Active Directory** is selected earlier, **You have selected Active Directory domain:** page displays.

11. Select **Create User Group EventTracker** or **Select existing User Group** option, and then select the **Next >** button.

NOTE:

When creating group,

- We encourage users to use the group name as 'EventTracker', though EventTracker works with any group name.

- In case this group name does not exist then the default choice will be to 'Create User Group EventTracker' else the default choice will be 'Select Existing Group'.

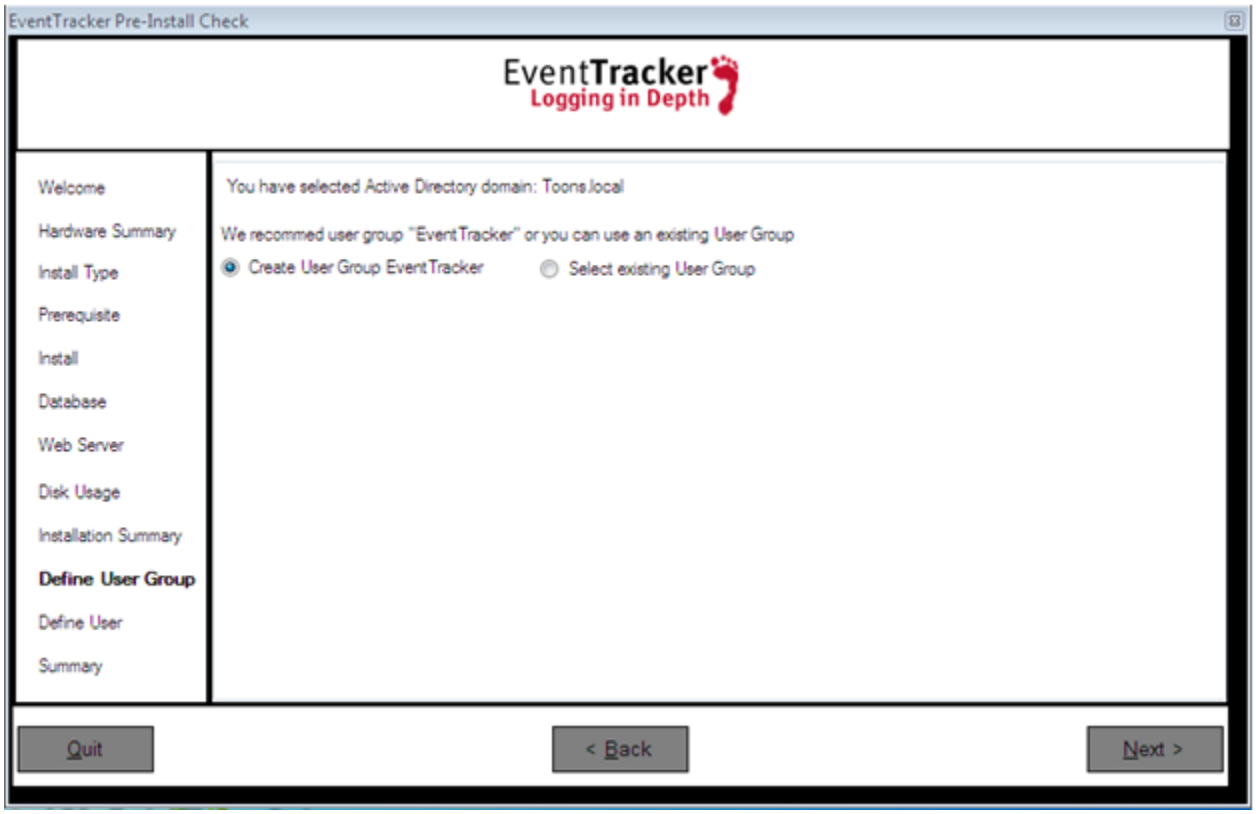


Figure 81

- If **Create User Group EventTracker** option is selected, then **Members of this User Group can access EventTracker** page displays.

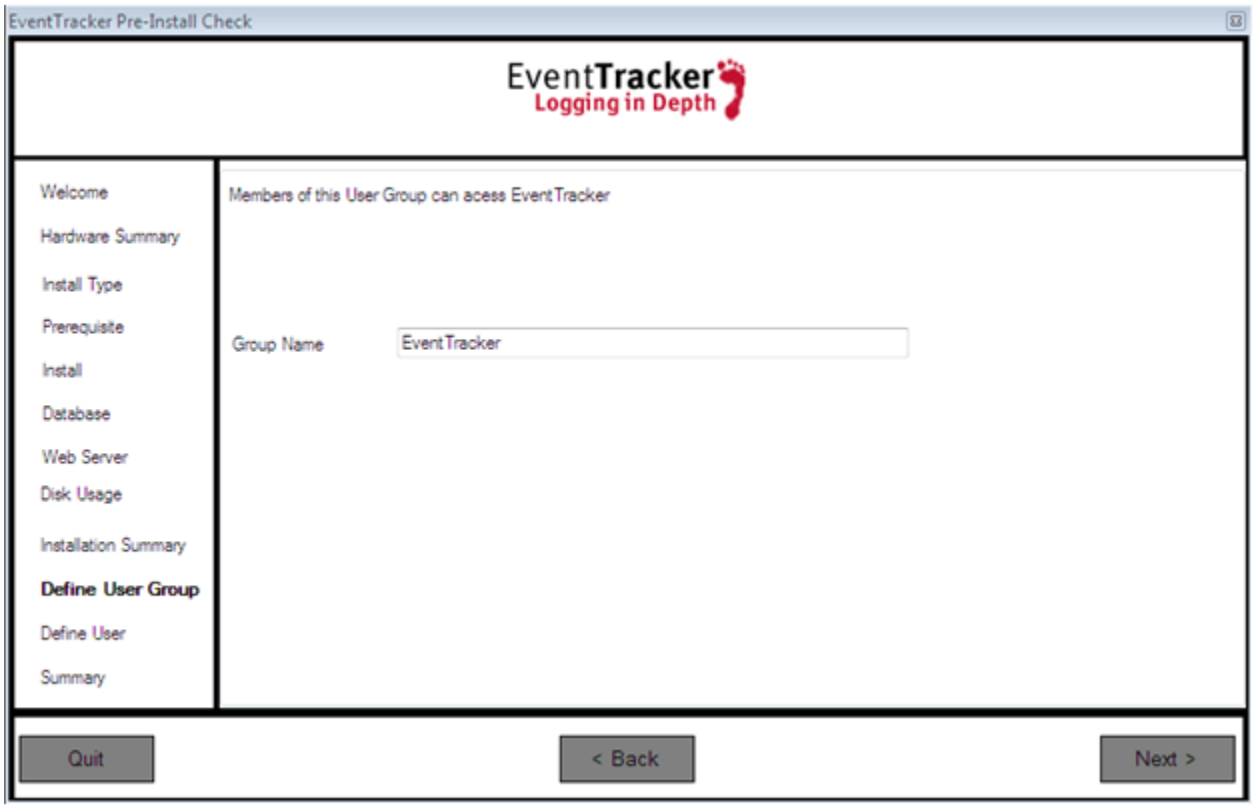


Figure 82

- Enter unique and appropriate **Group Name,** and then click the **Next >** button.

NOTE:

If user does not have appropriate permissions to create a group on the Active Directory machine, then error message 'Access Denied' displays. Please contact administrator if you do not have sufficient permissions.

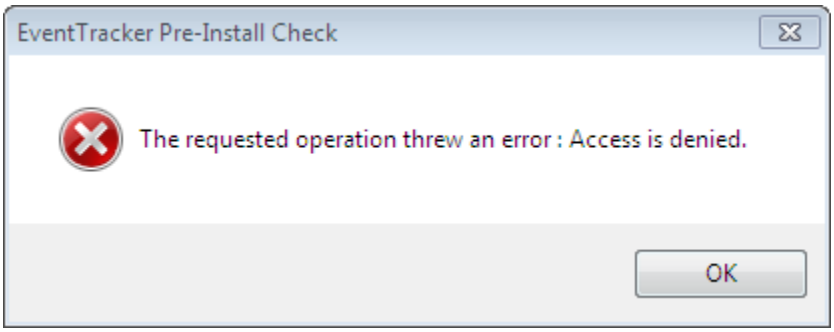


Figure 83

A. Click the **OK** button.

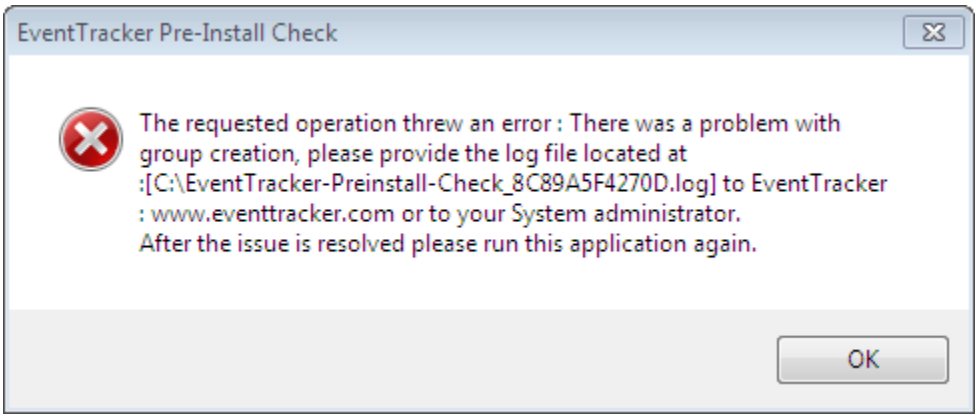

EventTracker Pre-Install Check
The requested operation threw an error : There was a problem with group creation, please provide the log file located at :[C:\EventTracker-Preinstall-Check_8C89A5F4270D.log] to EventTracker : www.eventtracker.com or to your System administrator.
After the issue is resolved please run this application again.
OK

Figure 84

- If **Select existing User Group** option is selected,

  a. Select any group, and then select the **Next >** button.

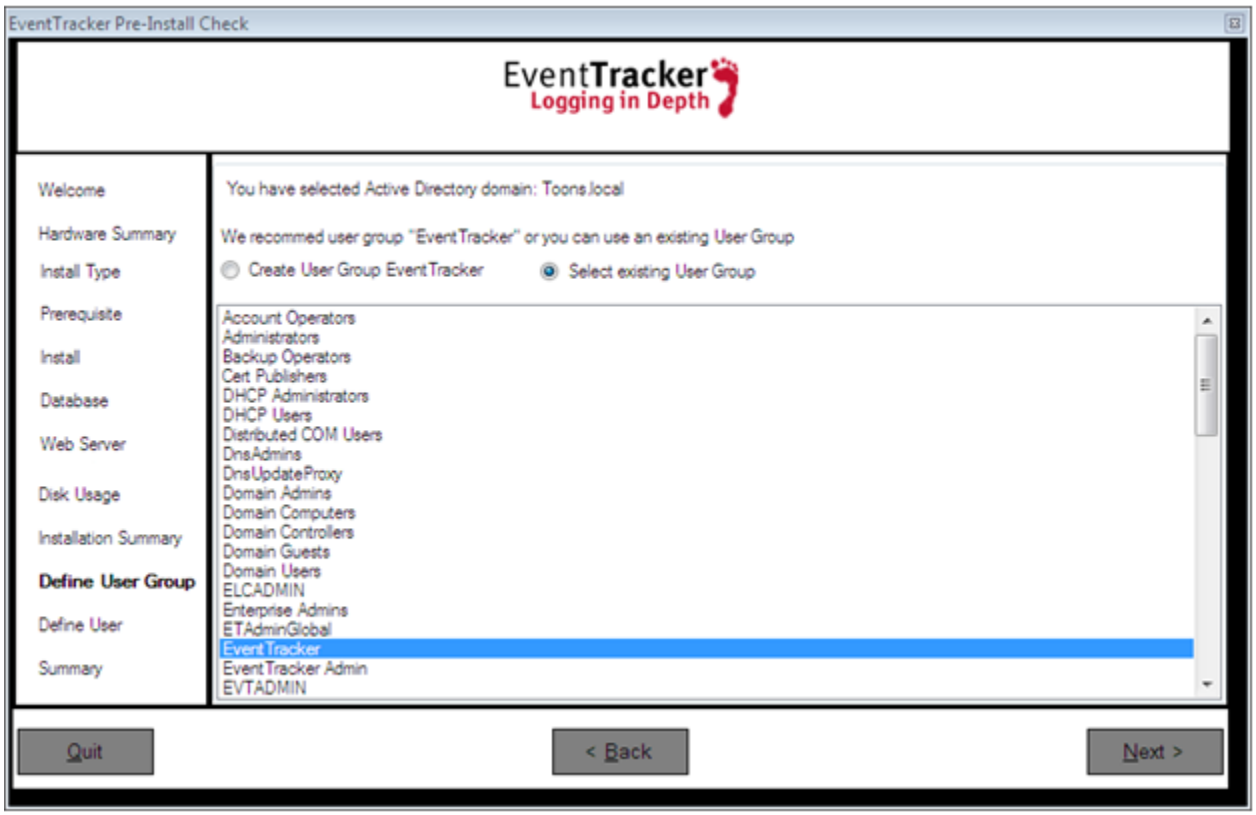


Figure 85

Define User page displays.

12. Select **Create EventTrackerAdmin/Find User/Select existing User** option.

❖ If **Create EventTrackerAdmin** option is selected, please refer Figure 85.

NOTE:

Administrator should have sufficient privileges on Active Directory machine as well as to create a group.

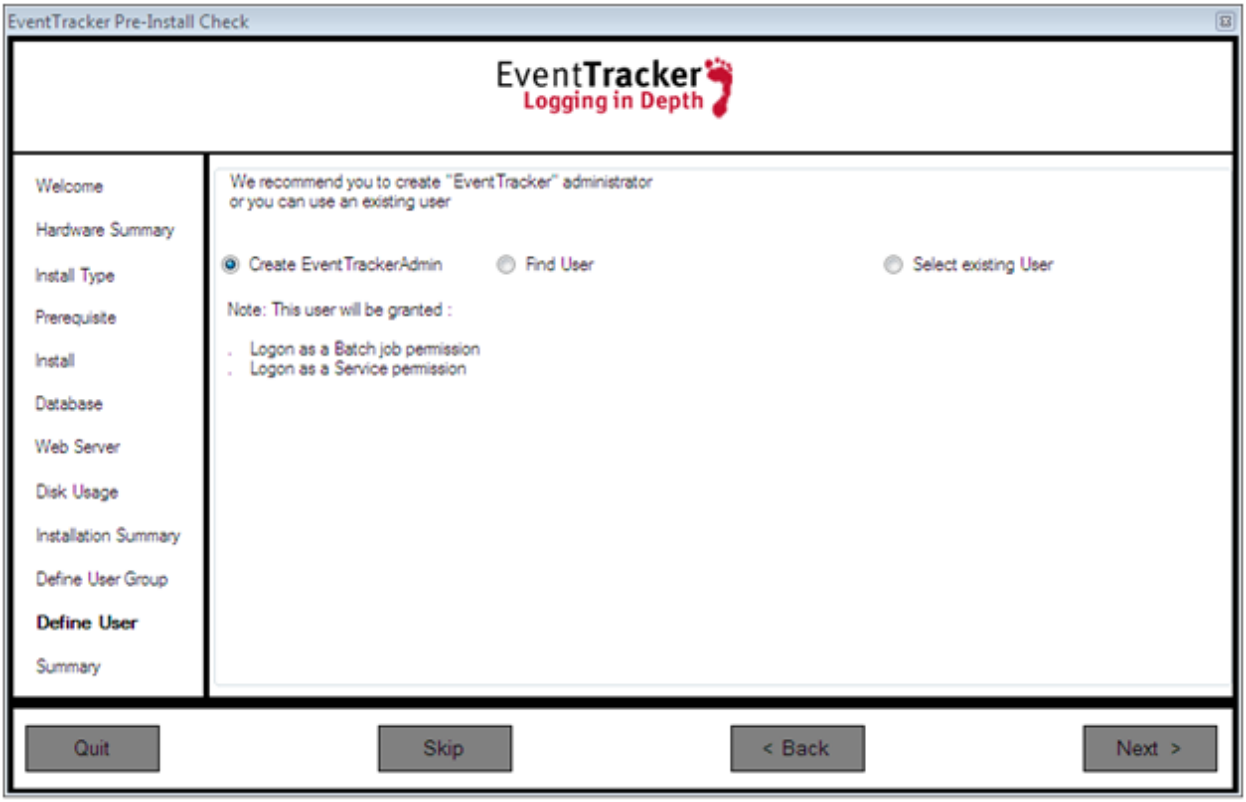


Figure 86

a. Click the **Next >** button.

This User will manage EventTracker page displays.

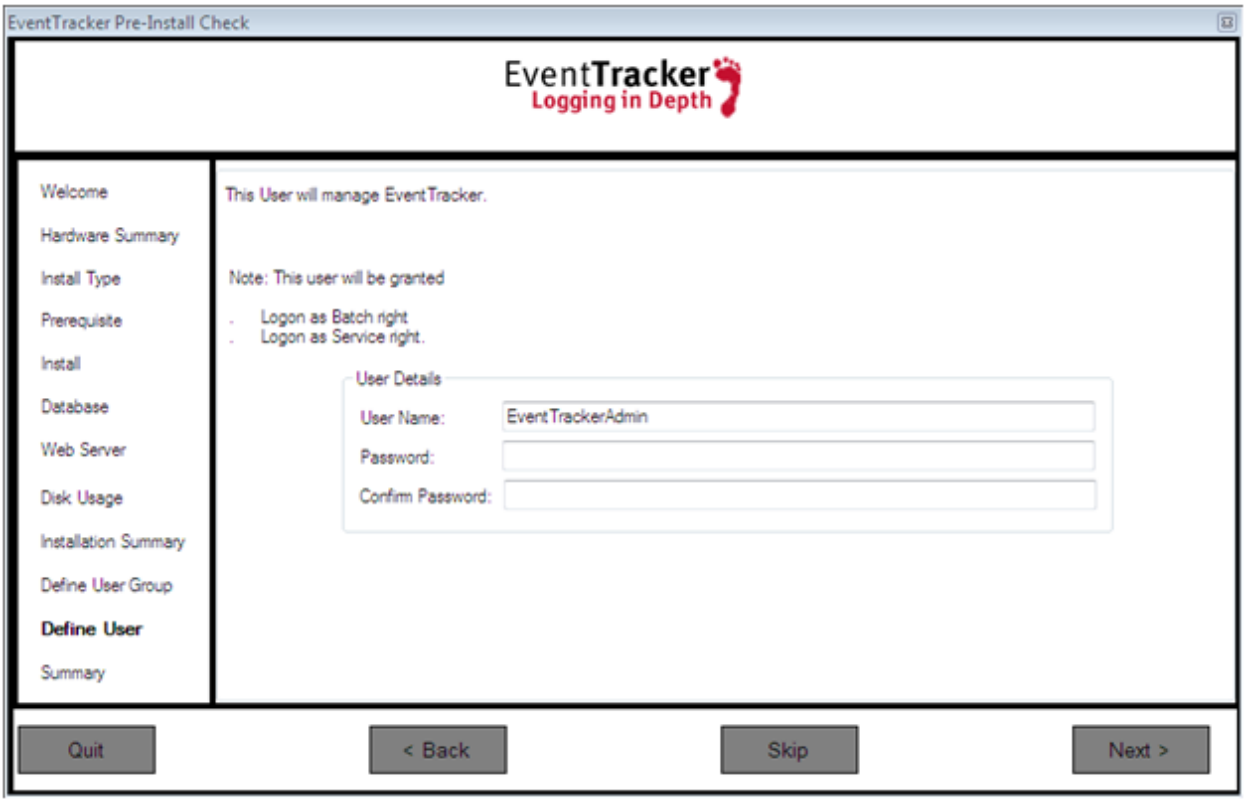


Figure 87

b. Enter relevant credentials, and then click the **Next >** button.

Summary page displays.

❖ If **Find User** option is selected,

a. Enter a name in the box, and then click the **Find** button.

NOTE:

A wildcard can also be entered.

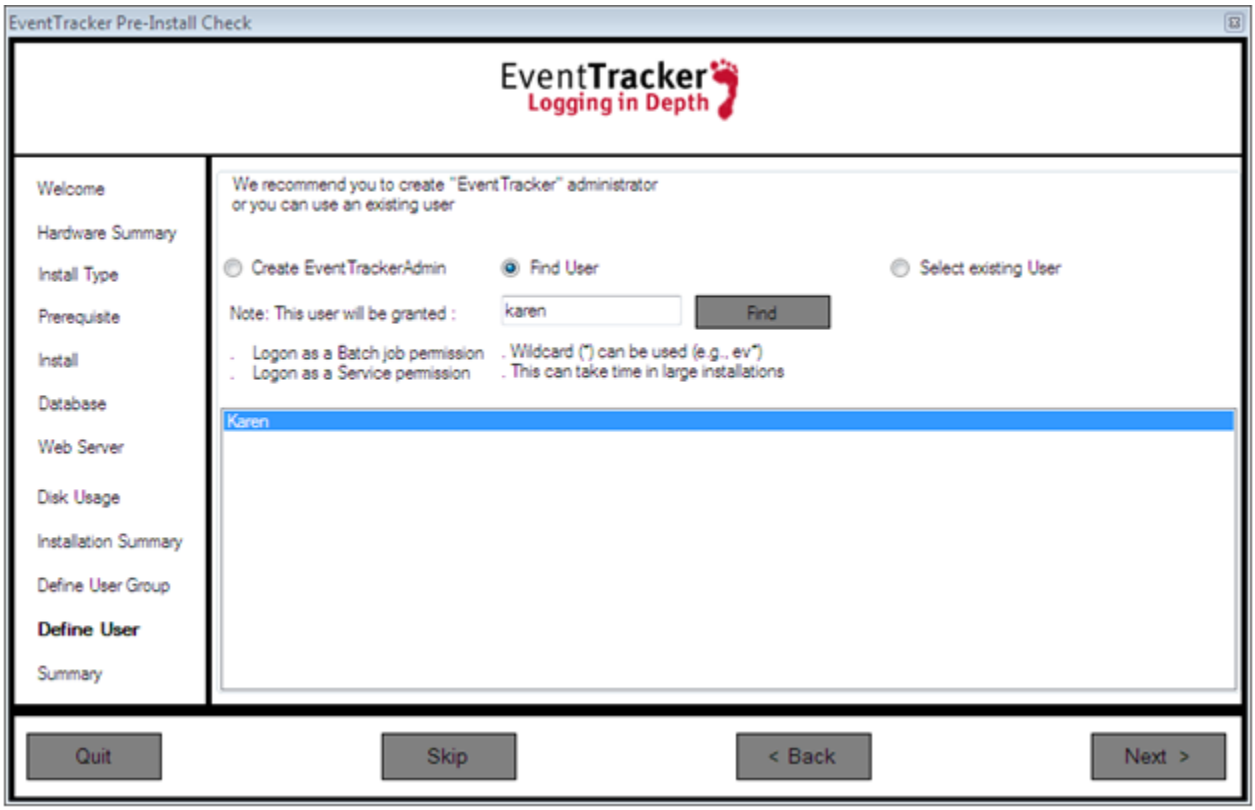


Figure 88

b. Click the **Next >** button.

   Summary page displays.

❖ If **Select existing User** option is selected, select an appropriate user, and then select the **Next >** button.

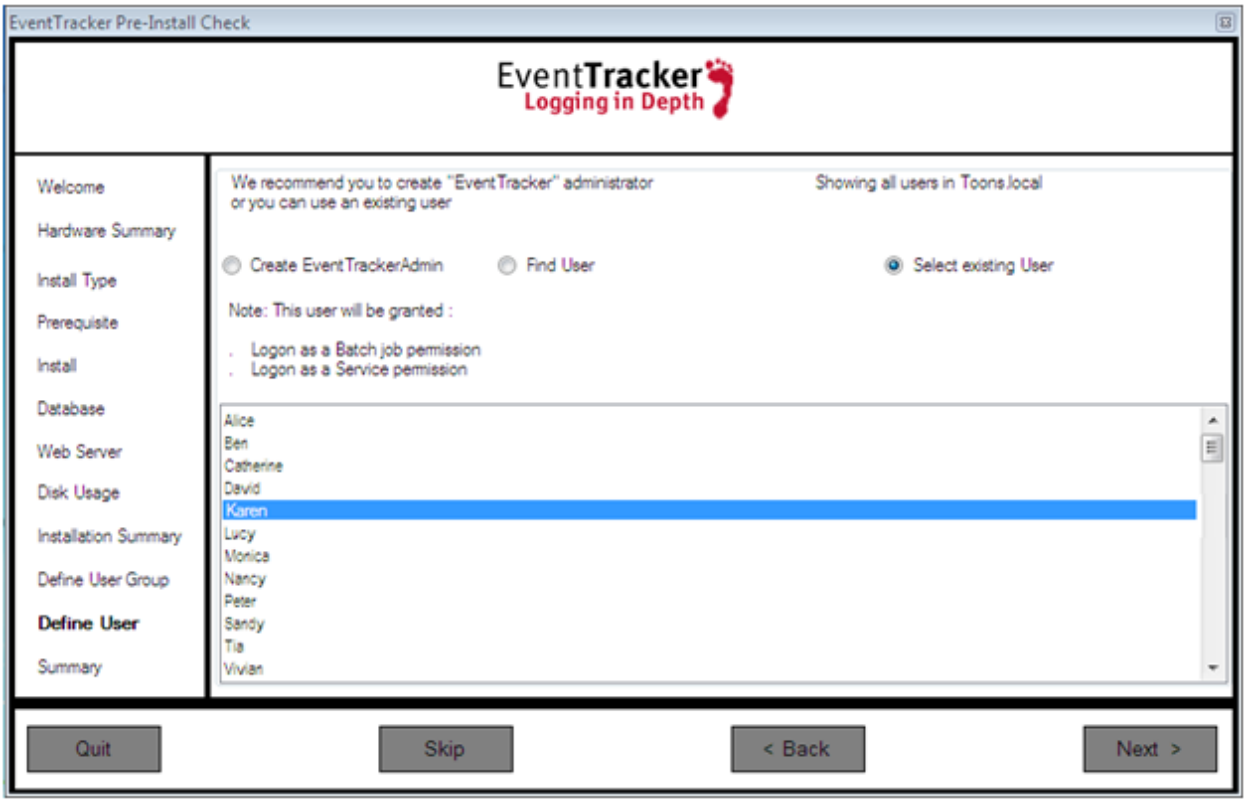


Figure 89

Summary page displays.

If user is not EventTracker Administrator then below message displays.

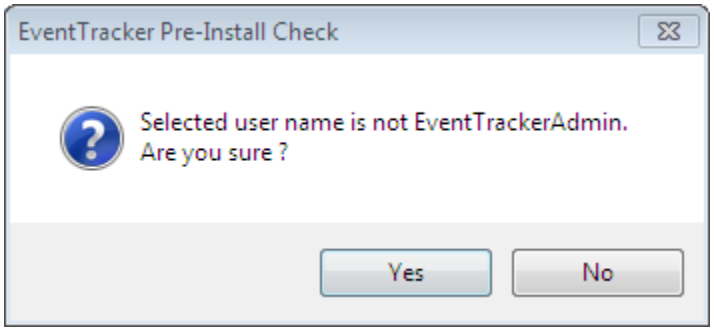


Figure 90

a. Click the **Yes** button.

13. In **Summary** page, verify all the data entered, and then click the **Install** button.

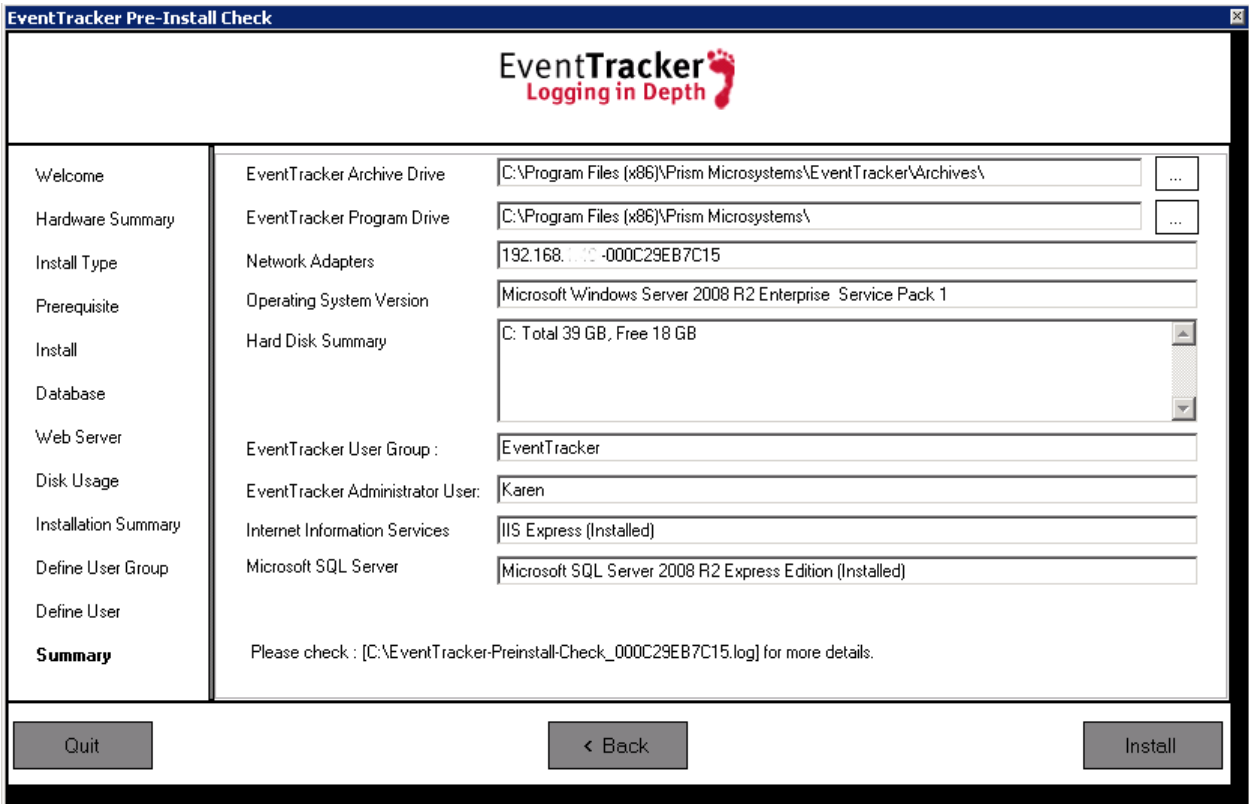


Figure 91

EventTracker Pre-Install Check window displays a message to confirm and proceed with installation of EventTracker.

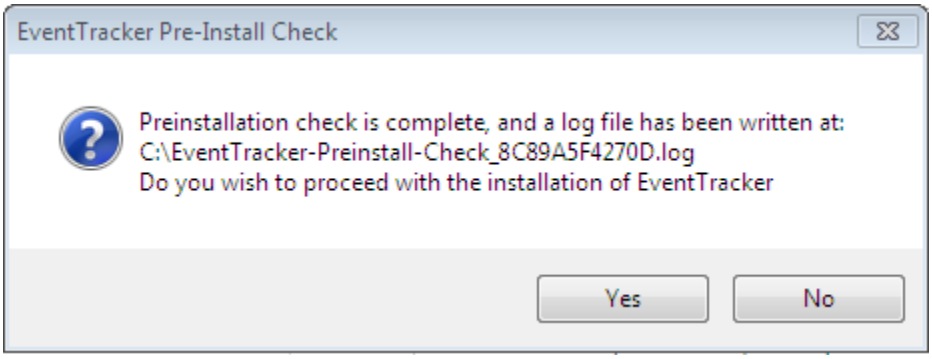

EventTracker Pre-Install Check
Preinstallation check is complete, and a log file has been written at:
C:\EventTracker-Preinstall-Check_8C89A5F4270D.log
Do you wish to proceed with the installation of EventTracker
Yes
No

Figure 92

14. Click the **Yes** button.

    InstallShield Wizard displays the **Welcome** screen.

EventTracker 7.5
7.5
EventTracker
Logging In Depth
Welcome to EventTracker Setup Program.
This setup program will install EventTracker on your computer. To continue, click Next.
WARNING: This program is protected by copyright law and international treaties.
Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.
© Copyright 1999-2014 Prism Microsystems, Inc.
< Back
Next >
Cancel

Figure 93

15. Click **Next >**.

    InstallShield Wizard displays the **License Agreement** screen.

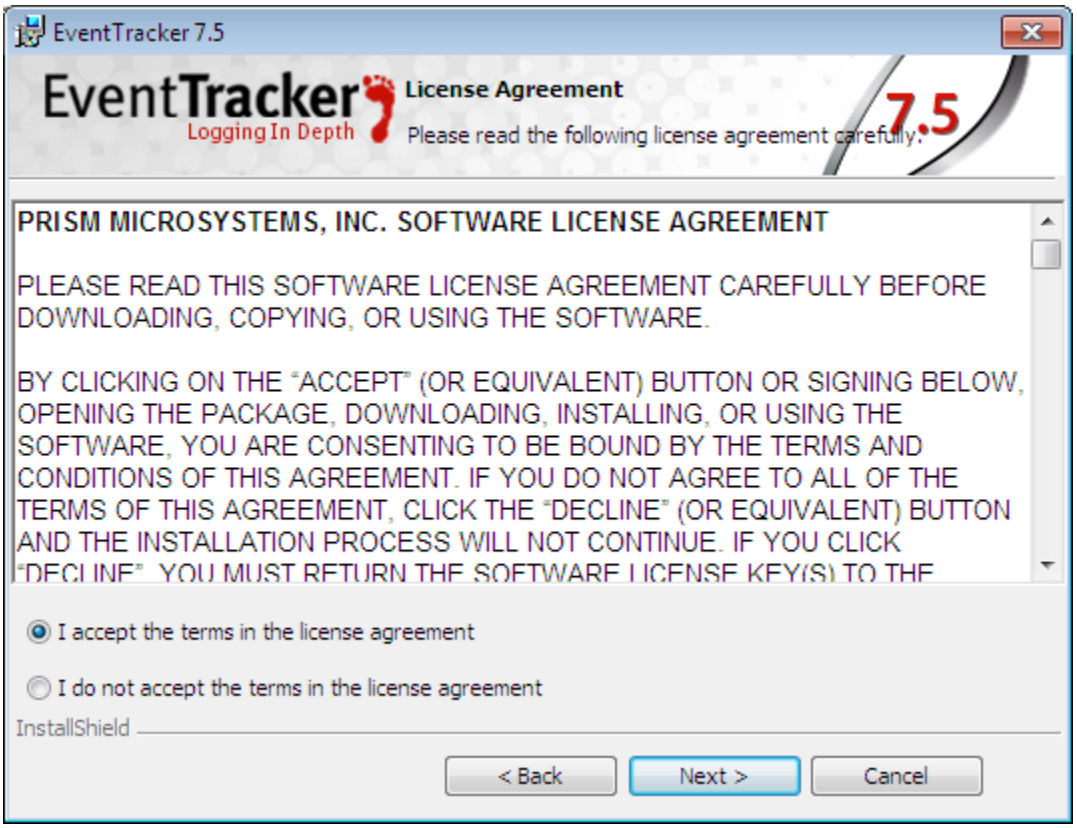

EventTracker 7.5
EventTracker
Logging In Depth
License Agreement
Please read the following license agreement carefully.
7.5
PRISM MICROSYSTEMS, INC. SOFTWARE LICENSE AGREEMENT
PLEASE READ THIS SOFTWARE LICENSE AGREEMENT CAREFULLY BEFORE DOWNLOADING, COPYING, OR USING THE SOFTWARE.
BY CLICKING ON THE "ACCEPT" (OR EQUIVALENT) BUTTON OR SIGNING BELOW, OPENING THE PACKAGE, DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU ARE CONSENTING TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE "DECLINE" (OR EQUIVALENT) BUTTON AND THE INSTALLATION PROCESS WILL NOT CONTINUE. IF YOU CLICK
I accept the terms in the license agreement
I do not accept the terms in the license agreement
InstallShield
< Back
Next >
Cancel

Figure 94

16. Read the license agreement, and then click '**I accept the terms in the license agreement**' option to accept the terms and condition.
17. Click the **Next >** button.

    Select a Certificate File page displays.

    NOTE:

    If the user has selected **Custom** option in EventTracker Pre Install Check, then the installer prompts to add the certificate file.

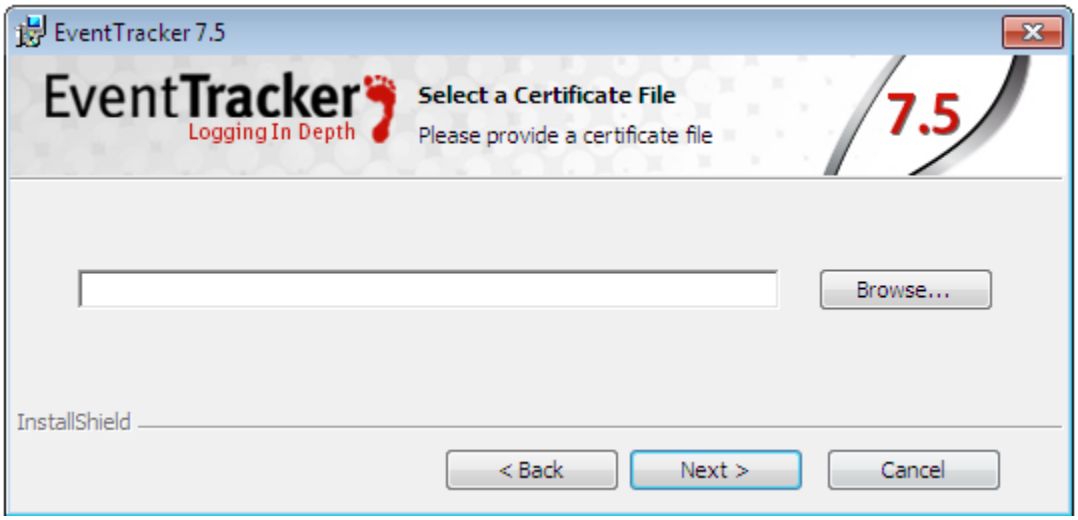


Figure 95

18. To locate the path of the certificate file, click the **Browse** button.

    InstallShield Wizard displays the **Select File** window.

19. Go to the appropriate folder, and then select the file.

20. Click **Open**.

    InstallShield Wizard updates the folder path.

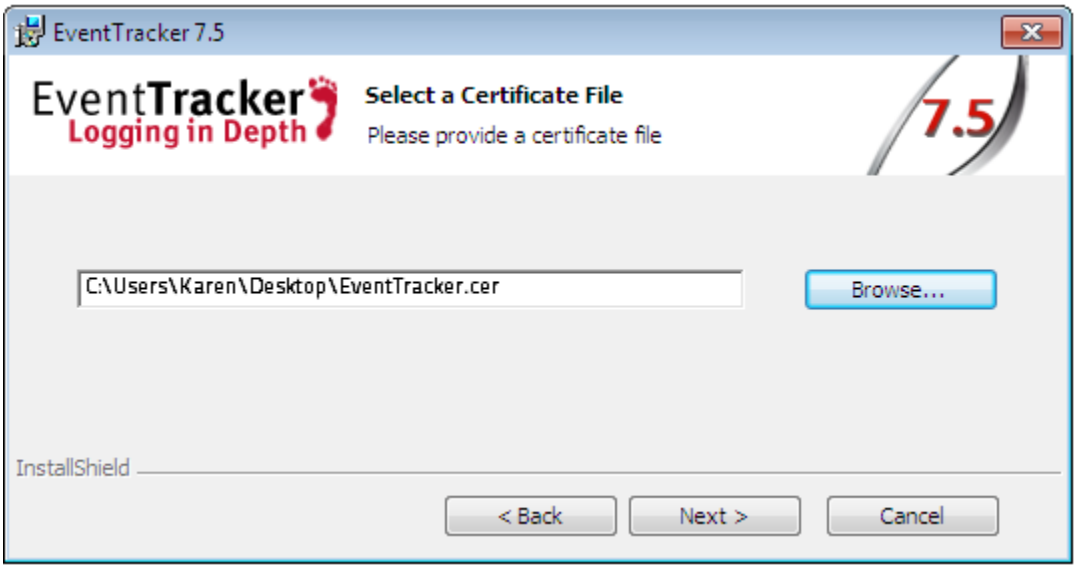


Figure 96

21. Click **Next >**.

    InstallShield[R] Wizard displays the **Select Components** screen.

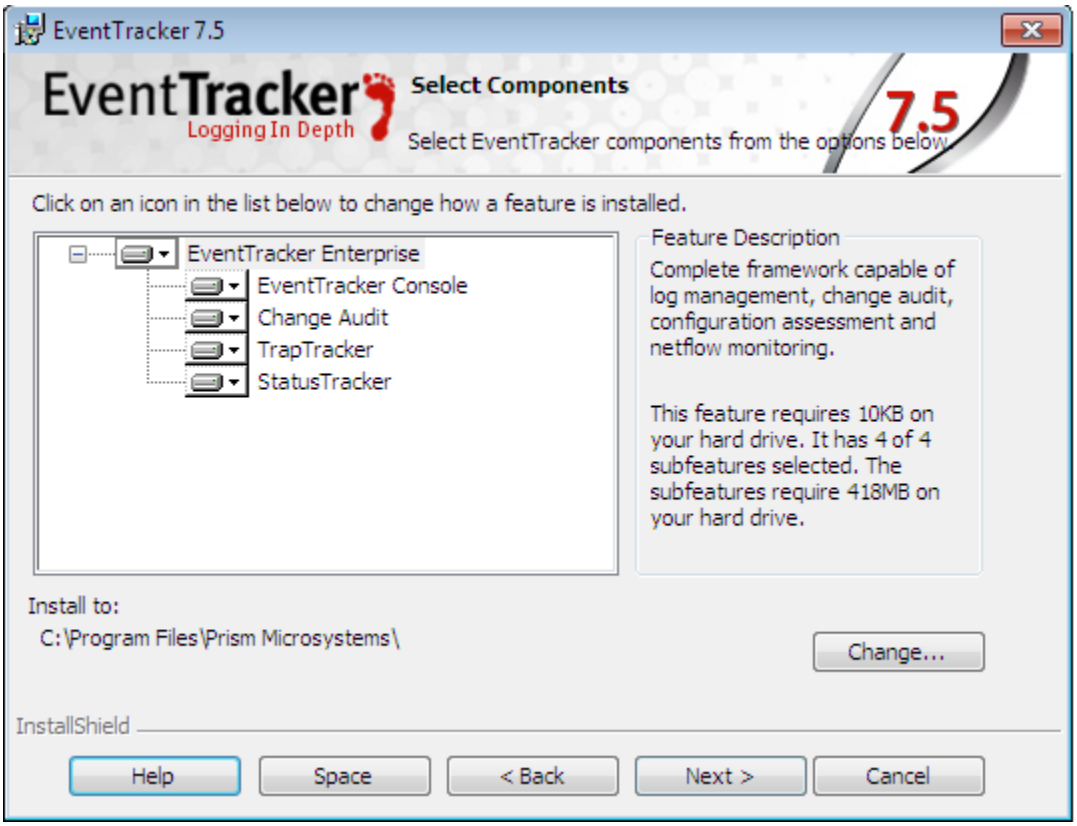
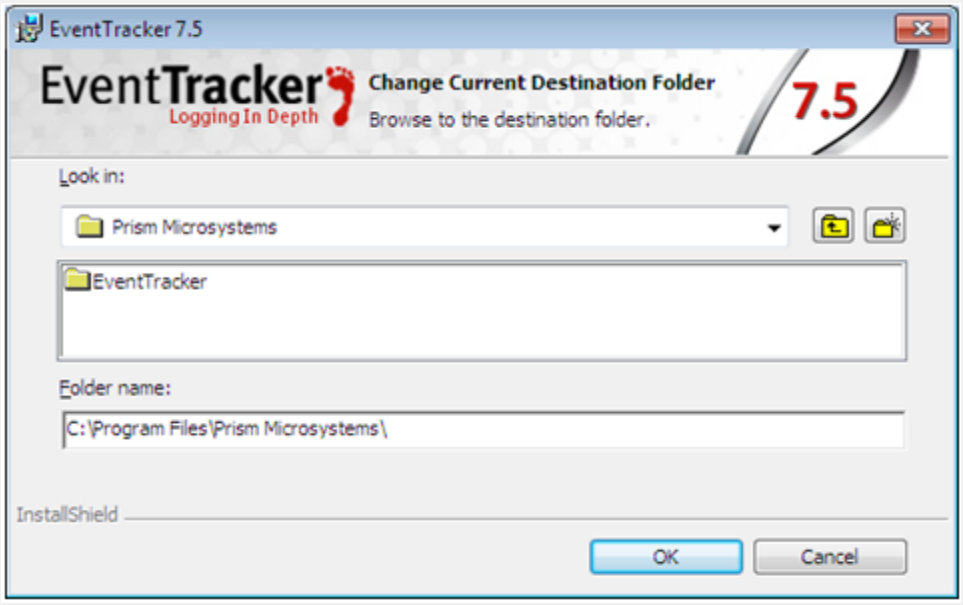
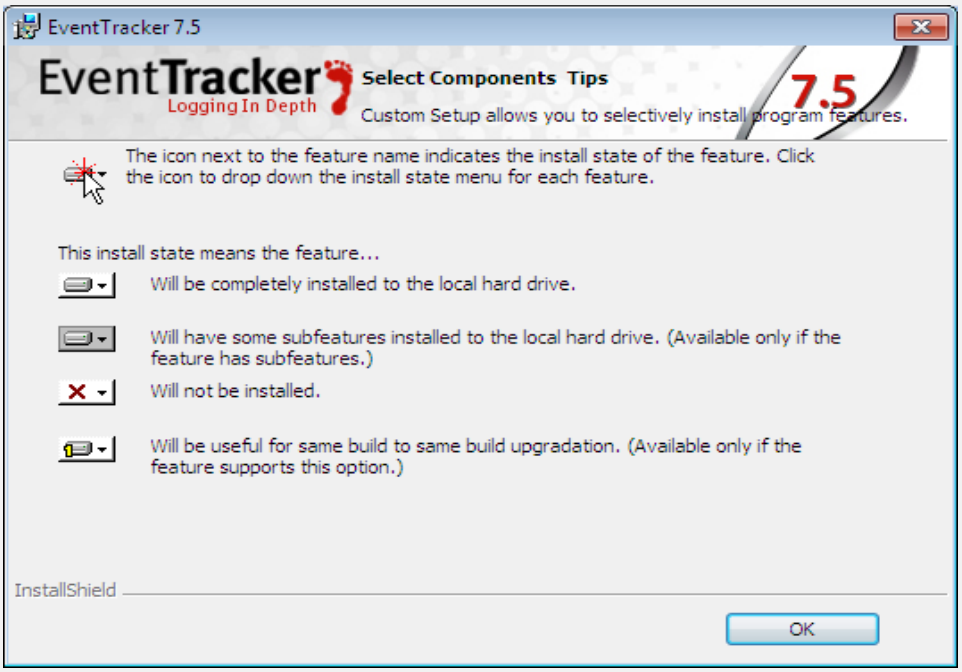
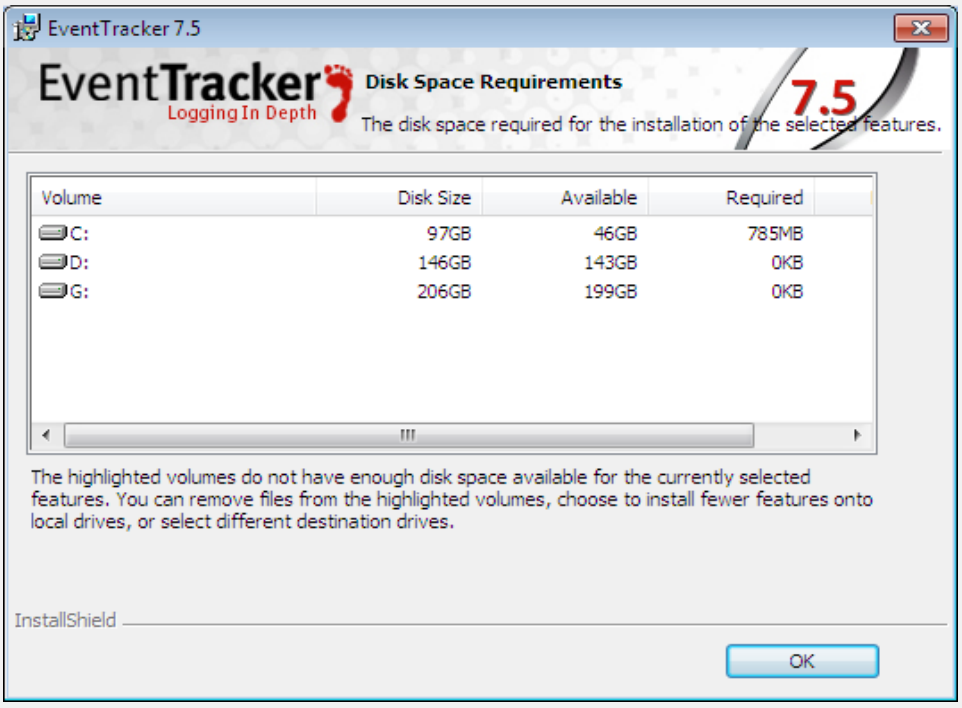

EventTracker 7.5
EventTracker
Logging In Depth
Select Components
Select EventTracker components from the options below
7.5
Click on an icon in the list below to change how a feature is installed.
EventTracker Enterprise
EventTracker Console
Change Audit
TrapTracker
StatusTracker
Feature Description
Complete framework capable of log management, change audit, configuration assessment and netflow monitoring.
This feature requires 10KB on your hard drive. It has 4 of 4 subfeatures selected. The subfeatures require 418MB on your hard drive.
Install to:
C:\Program Files\Prism Microsystems\
Change...
InstallShield
Help
Space
< Back
Next >
Cancel

Figure 97

EventTracker Components	Description
EventTracker Console	Select this option to install manager console on target computer.
Change Audit	Optional component. Installing this component enables you to monitor and manage change over the enterprise. Agent component will also be installed along with the Manager Console. You can also deploy agent to the monitored computers using System Manager after installing the Manager Console.
Trap Tracker	Optional component. Installing this component enables you to monitor and manage traps sent by SNMP compliant devices.

Status Tracker	Optional component. Installing this component enable you to monitor and manage TCP/IP networks, Web sites, applications, and ports in mission critical environment.

Click	To
Change...	Select different destination folder to install EventTracker. 

Help	View **Select Component** conventions. 
Space	Check the disk space available in the target computer. 

22. Click **Next** >.

InstallShield Wizard displays the **Select EventTracker Console Type** screen.

Standard Console:

Best for flat network topologies where all monitored nodes report directly to one (or redundant) EventTracker Console.

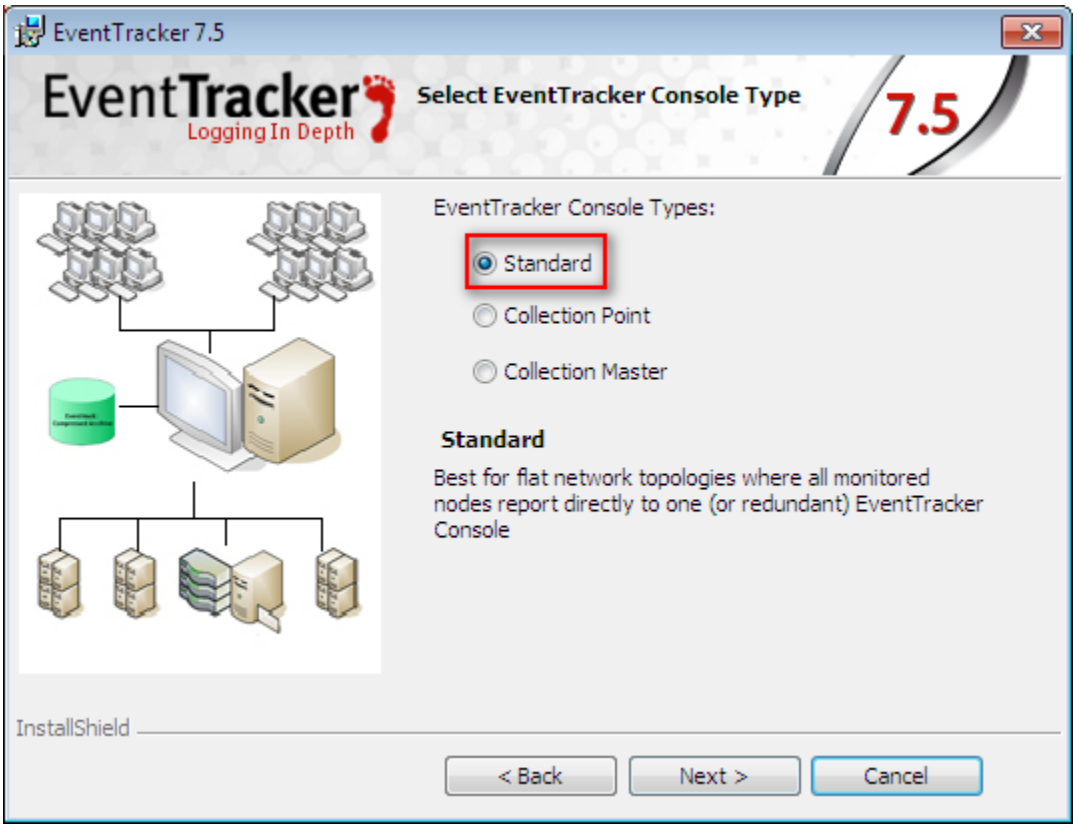


Figure 98

Collection Point:

Used in hierarchical network topologies where monitored nodes report to a local EventTracker Console which in turn replicates its event log archive to a Collection Master.

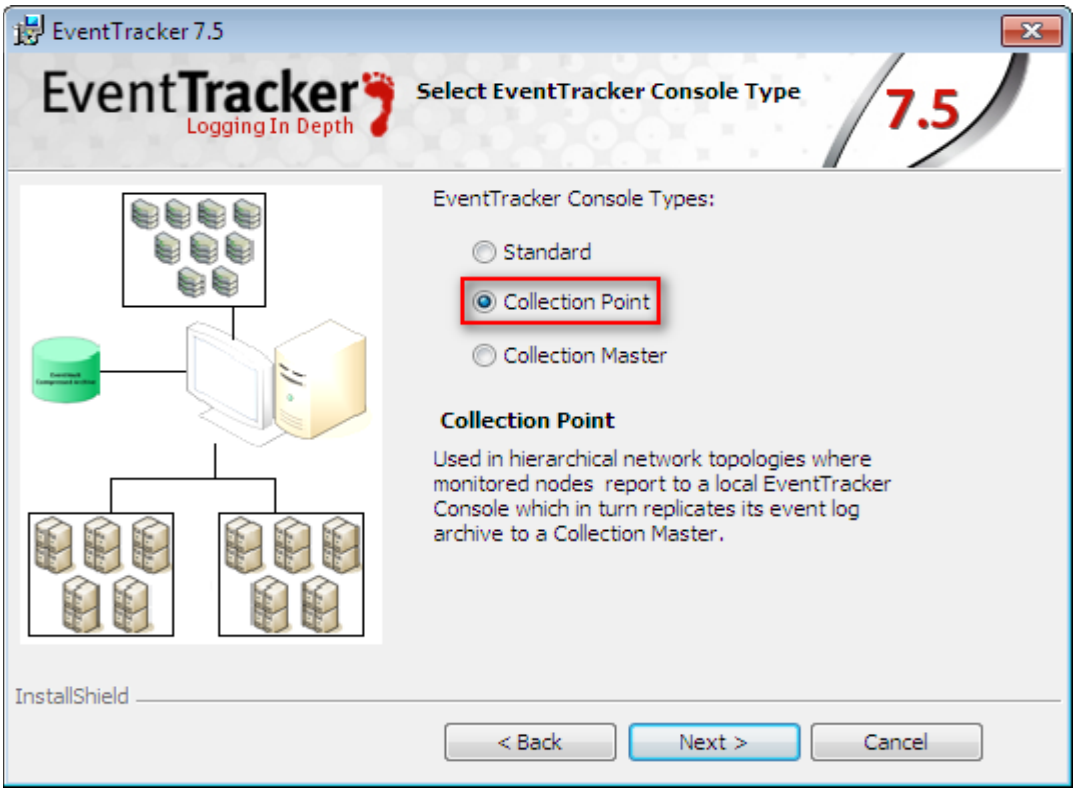


Figure 99

a) Select the console type as **Collection Point**, and then click **Next >**.

InstallShield Wizard displays **Configure Collection Point site** page.

b) Enter **Site name:** and then select the **Next >** button.

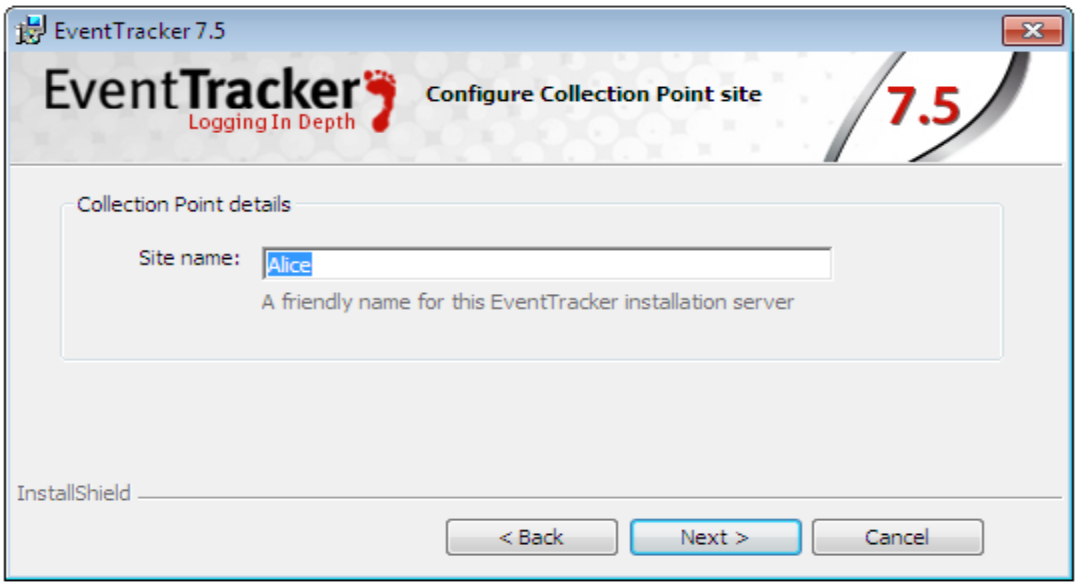


Figure 100

NOTE:
Some special characters are not allowed while providing site/group name. InstallShield[R] Wizard will display a pop-up window if site or group name is provided with such special characters.

Figure 101

Collection Master:

Used in hierarchical network topologies where collection points replicate their event log archives to a Collection Master.

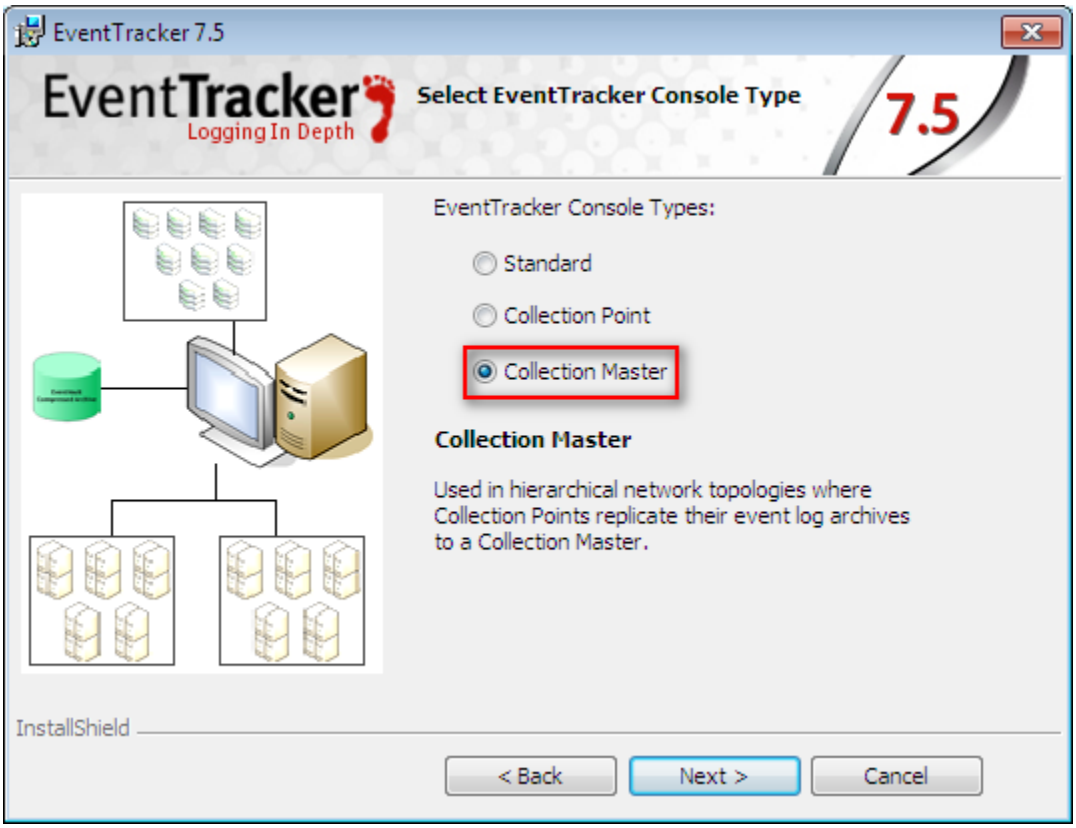


Figure 102

23. Select a console type, and then click **Next >**.

    If you have selected **Change Audit** component, then InstallShield[R] Wizard displays **Change Audit SnapShot** dialog box.

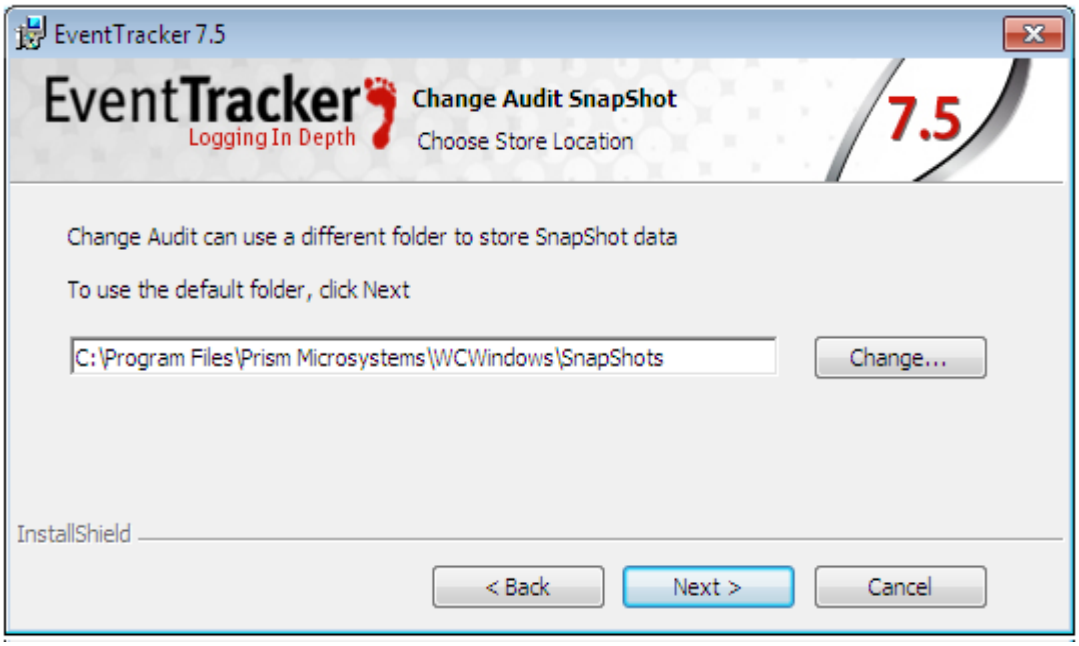


Figure 103

24. Click the **Next >** button to keep the default store location.

    (OR)

    Click the **Change** button to change the snapshot store location.

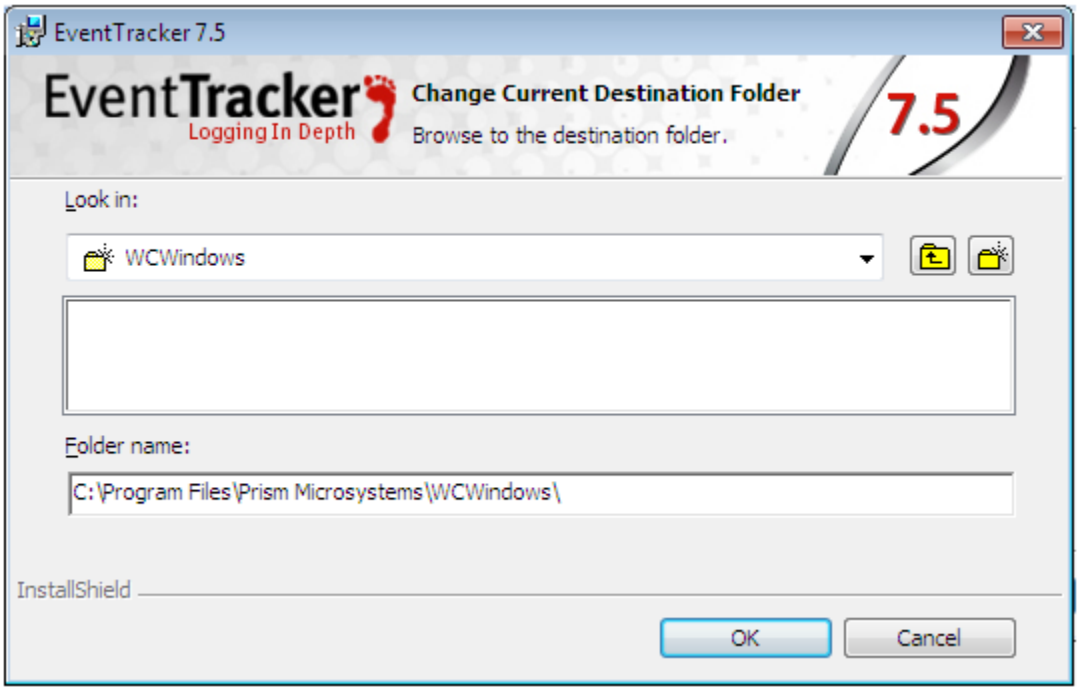


Figure 104

25. Browse the destination folder, and then click the **OK** button.

NOTE:

The Change Audit snapshot store location can be changed only during fresh install and if snapshots are not retained during uninstall.

In case of upgrade, if the change audit snapshots are retained during product un-installation, then the snapshot store location path cannot be changed.

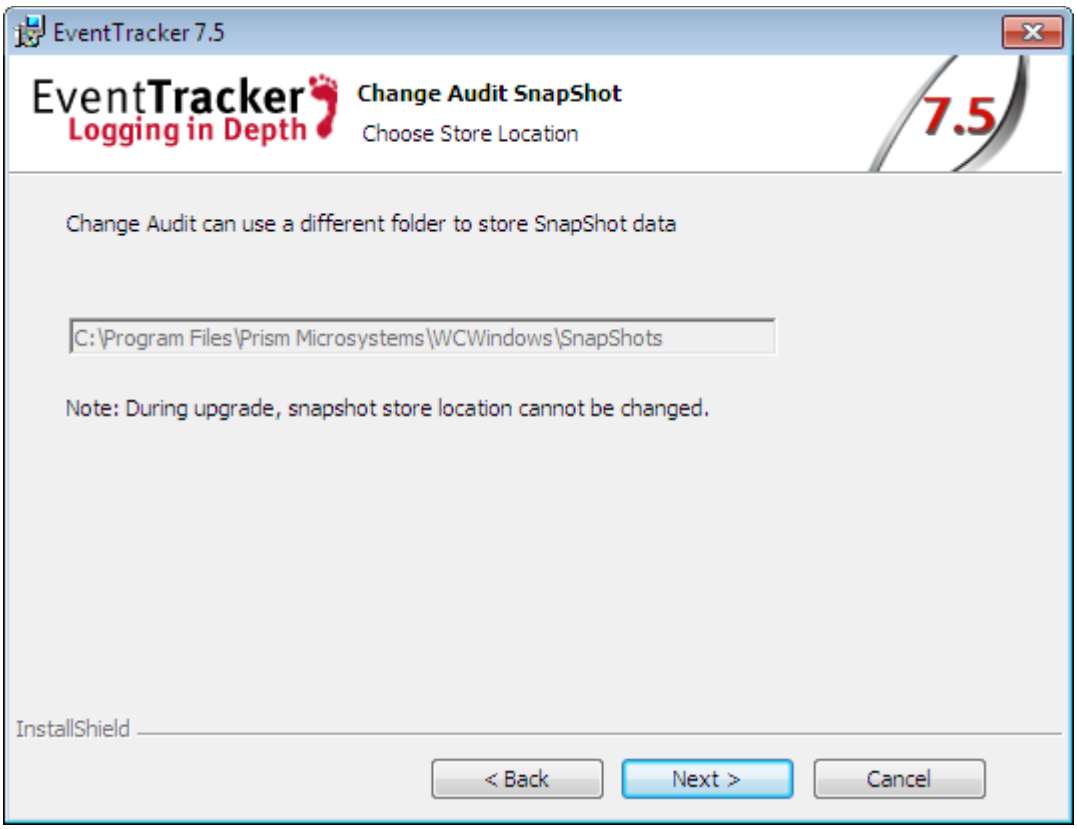


Figure 105

If you have not selected to install **Change Audit,** then InstallShield[R] Wizard displays the **Ready to Install the Program** screen.

26. Select the **Install Remedial Action EXEs on this machine** option.

Remedial Action EXEs are copied to <InstallDir>\EventTracker\Agent\Script folder.

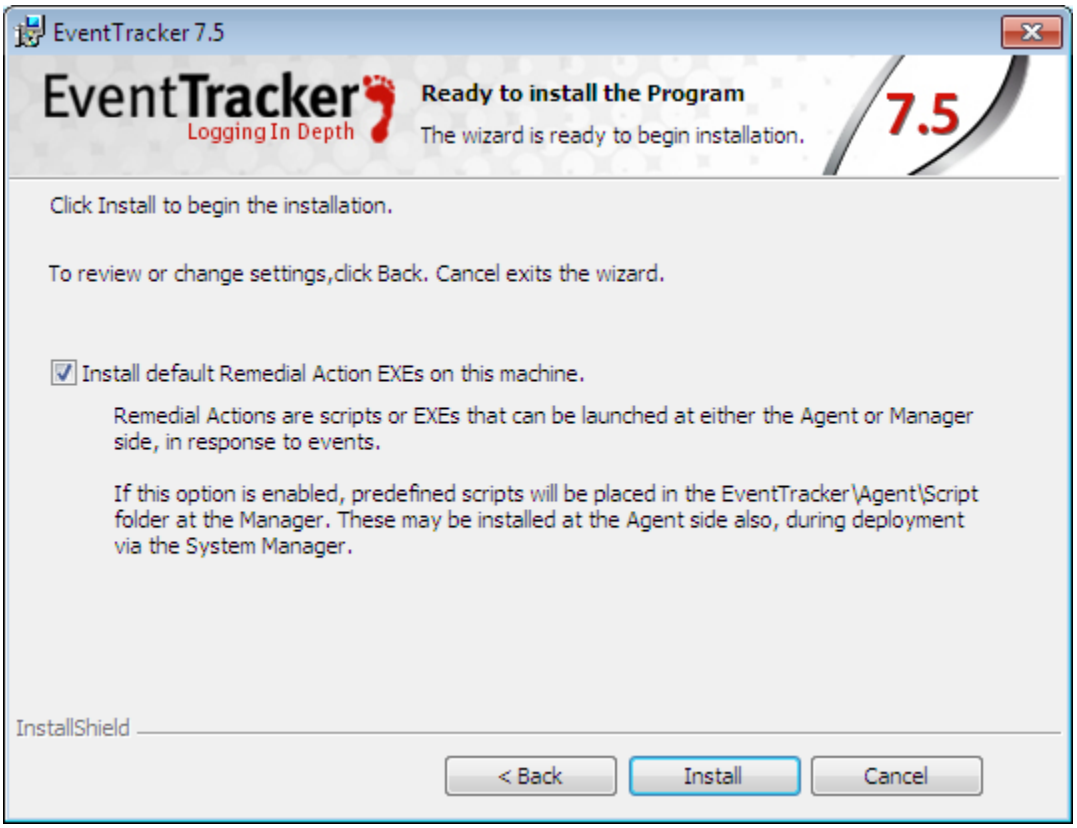

EventTracker 7.5
EventTracker
Logging In Depth
Ready to install the Program
The wizard is ready to begin installation.
7.5
Click Install to begin the installation.
To review or change settings,click Back. Cancel exits the wizard.
Install default Remedial Action EXEs on this machine.
Remedial Actions are scripts or EXEs that can be launched at either the Agent or Manager side, in response to events.
If this option is enabled, predefined scripts will be placed in the EventTracker\Agent\Script folder at the Manager. These may be installed at the Agent side also, during deployment via the System Manager.
InstallShield
< Back
Install
Cancel

Figure 106

27. Click the **Install** button.

    InstallShield Wizard installs the selected components.

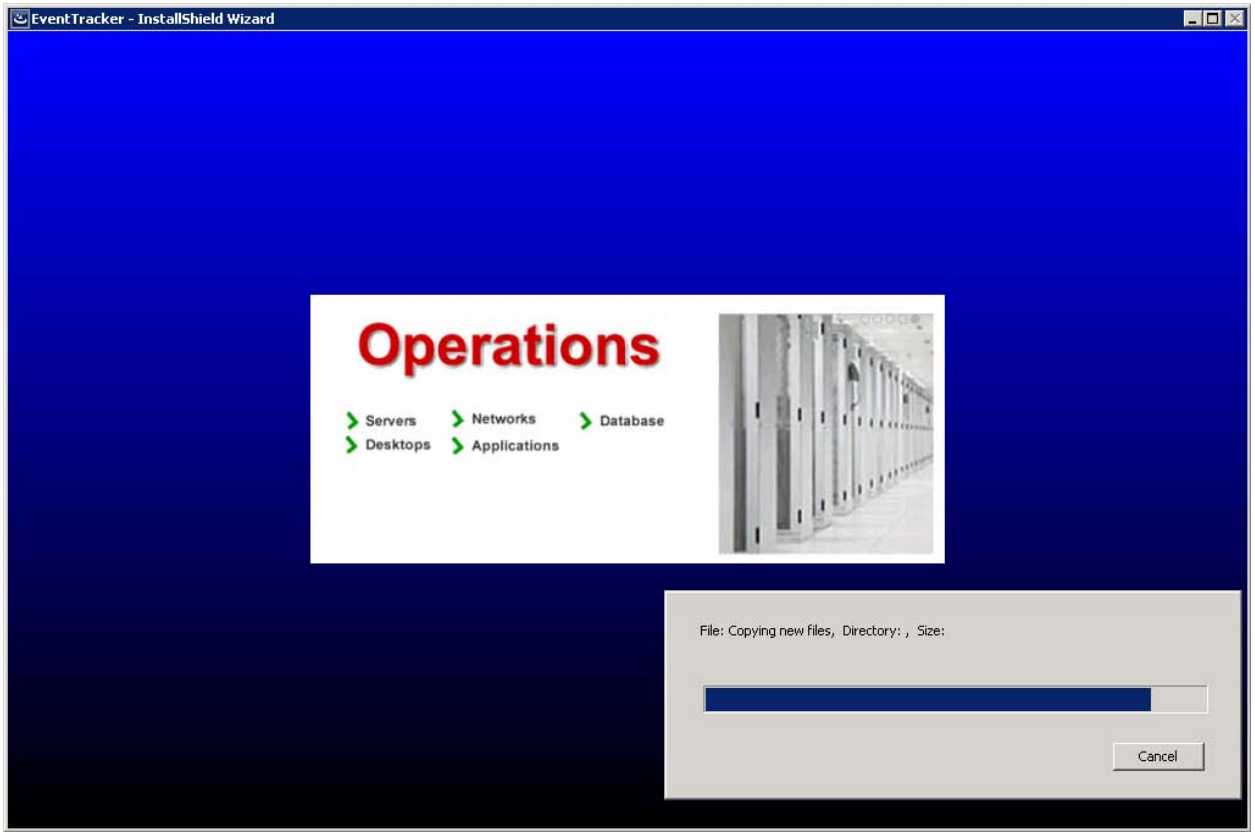


Figure 107

InstallShield Wizard initializes the configuration settings required for proper operation of EventTracker. After initializing the necessary configuration settings, InstallShield[R] Wizard displays the **Basic configuration** dialog box.

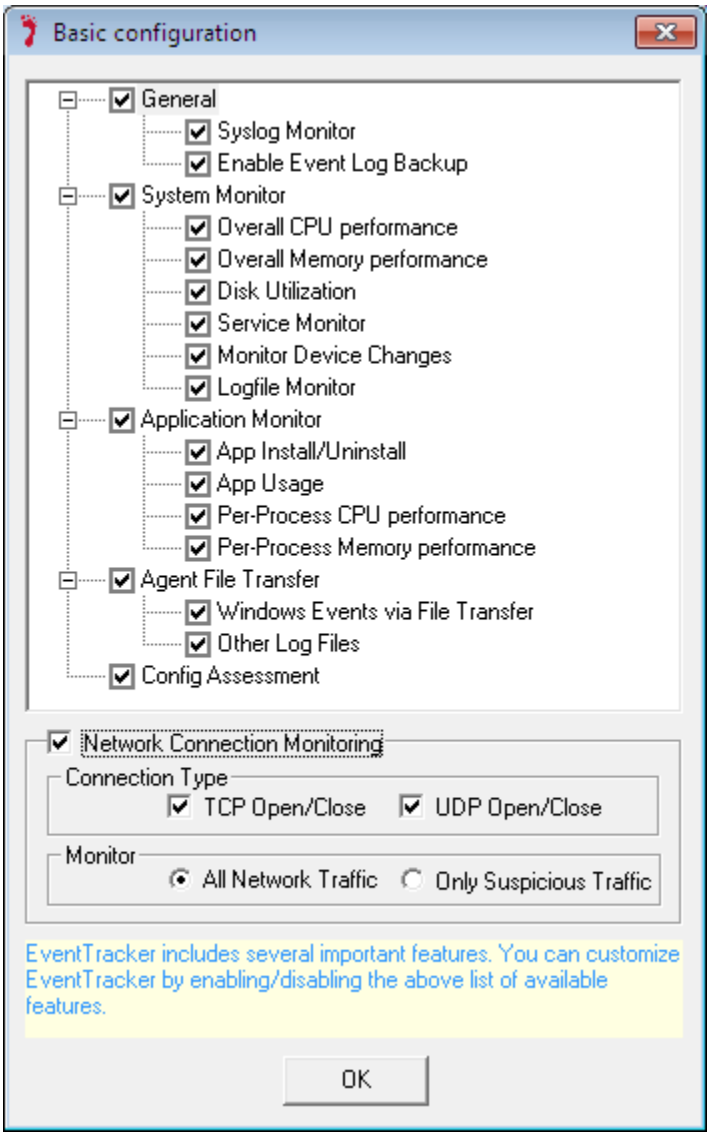


Figure 108

28. Select appropriate options, and then click **OK**.

    InstallShield Wizard displays the **Alert and Report generation settings** dialog box.

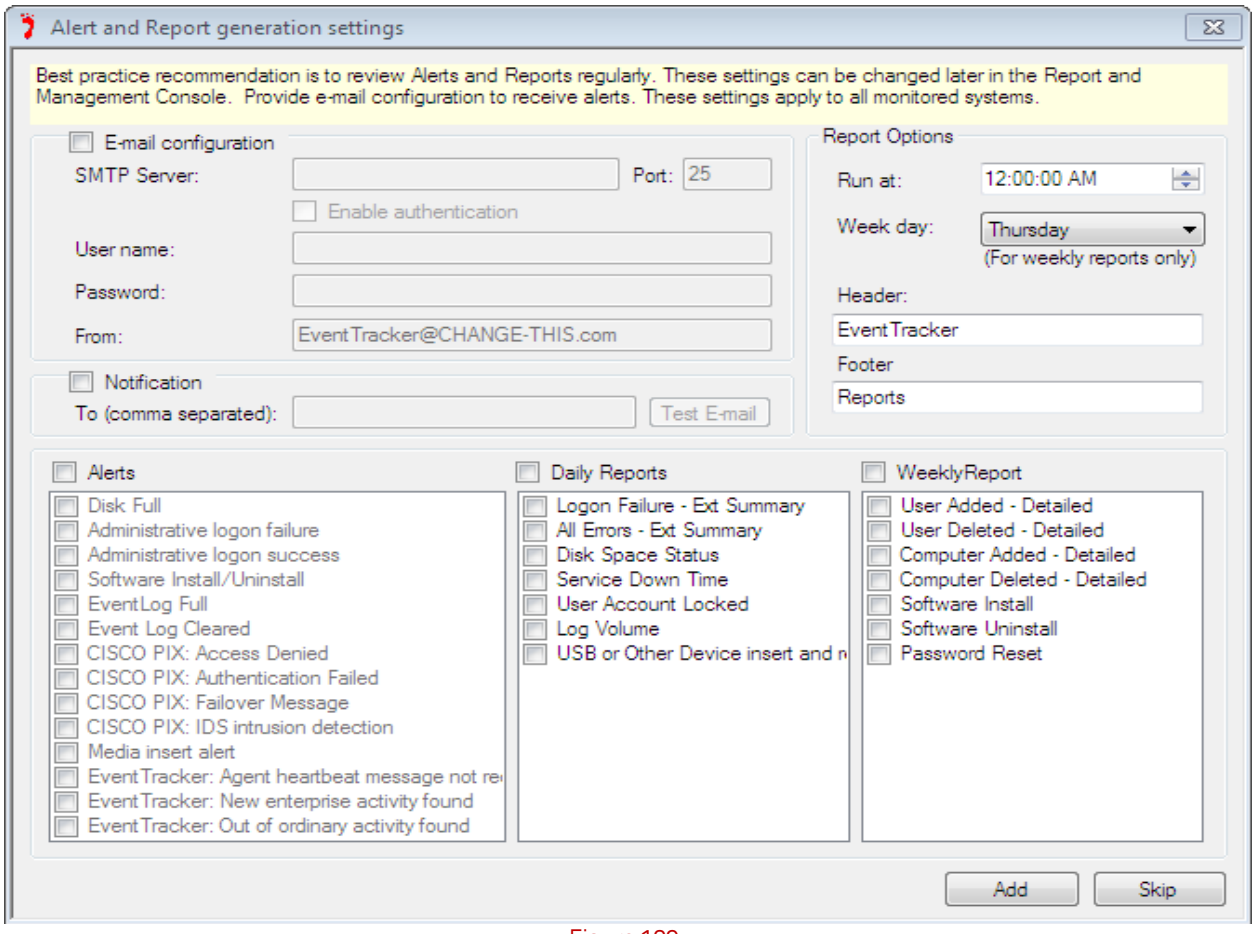


Figure 109

29. Select/enter appropriate data in the relevant fields, and then click **Add**.

    (OR)

    Click **Skip** if you do not wish to add the basic settings.

    InstallShield Wizard displays the last screen.

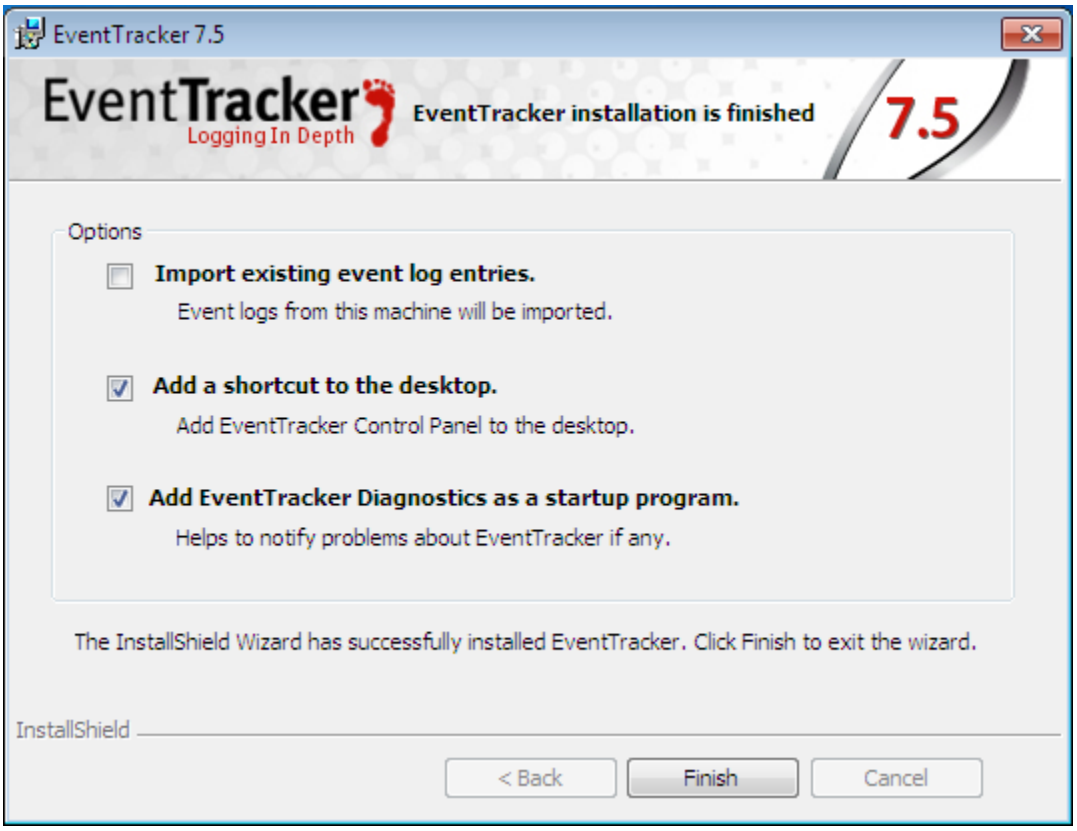

EventTracker 7.5
EventTracker
Logging In Depth
EventTracker installation is finished
7.5
Options
Import existing event log entries.
Event logs from this machine will be imported.
Add a shortcut to the desktop.
Add EventTracker Control Panel to the desktop.
Add EventTracker Diagnostics as a startup program.
Helps to notify problems about EventTracker if any.
The InstallShield Wizard has successfully installed EventTracker. Click Finish to exit the wizard.
InstallShield
< Back
Finish
Cancel

Figure 110

30. Click **Import existing event log entries** option to import event logs of EventTracker. Windows Security Alert message will be displayed if Firewall is on.

Windows Security Alert
To help protect your computer, Windows Firewall has blocked some features of this program.
Do you want to keep blocking this program?
Name: GetAllEvt PreVista Application
Publisher: Prism Microsystems, Inc
Keep Blocking
Unblock
Ask Me Later
Windows Firewall has blocked this program from accepting connections from the Internet or a network. If you recognize the program or trust the publisher, you can unblock it. When should I unblock a program?

Figure 111

Firewall blocks the incoming network connection, if getallevt.exe does not exist in the Program and Services Exceptions and displays a notification.

31. Click **Unblock** for the getallevt.exe to import event logs.
32. Check **Add a shortcut to the desktop** option, to add the shortcuts to the EventTracker application on the desktop.

    Add EventTracker diagnostics as a startup program option is selected by default to notify problems about EventTracker, if any.
33. Click **Finish** to conclude the installation process.

    InstallShield[R] Wizard displays the **EventTracker Configuration** screen.

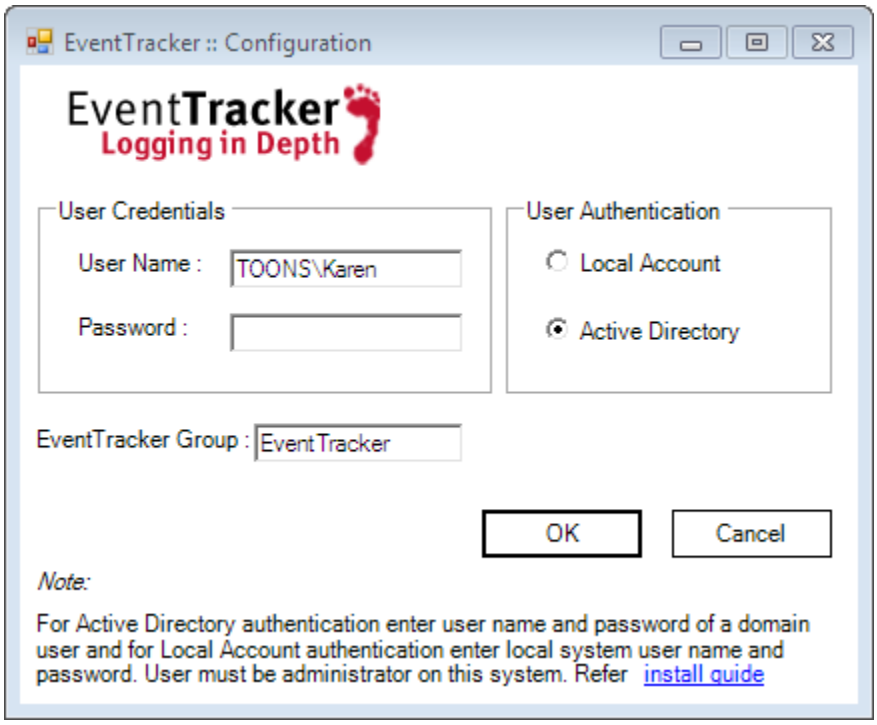


Figure 112

NOTE:
Make sure that you select/enter the correct **User Credentials, User Authentication and EventTracker Group** in order to login successfully. The user name/authentication that is done in EventTracker Preinstall Check, reflects in this screen, but user has the option to override it.

34. Type valid user credentials in the **User Name** and **Password** fields respectively.

    NOTE:

    EventTracker services run under this account. By default, this user is assigned the 'Event Tracker Administrator' role and can login to EventTracker.
35. Select a **User Authentication** option.

    Local Account: Authentication is done locally on the computer where EventTracker is being

installed.

Active Directory: Authentication is done in the Active Directory.

36. Type the EventTracker group name in the **EventTracker Group** field.
37. Click **OK**.

    After successfully validating the user credentials, InstallShield[R] Wizard displays the **EventTracker Configuration** message box.

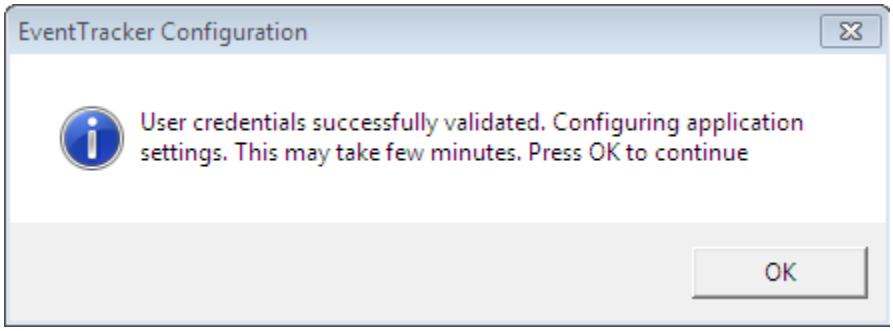

EventTracker Configuration
User credentials successfully validated. Configuring application settings. This may take few minutes. Press OK to continue
OK

Figure 113

38. Click **OK**.

    NOTE:

    If you change the system logon password, EventTracker logon password has to be updated. In order to synchronize the password, please update the same in **EventTracker Configuration.**

    i. To find '**EventTracker Configuration'**, select the **Start** button, select All **Programs**.

    ii. Select **Prism Microsystems**, select **EventTracker**, and then select **EventTracker Configuration.**

    iii. Enter appropriate credentials and then select the **OK** button**.**

Procedure to install EventTracker Manager v7.5.53 - Standard / Collection Point

NOTE:

If **Standard** or **Collection Point** is selected, then

- The archive path will be the drive with the maximum free space
- Local machine authentication will be used
- Group will be created as 'EventTracker'
- User name will be 'EventTrackerAdmin'
- This user will be local machine admin
- This user will be given 'Logon as batch user' rights, and 'Logon as Service' rights
- Only express versions of IIS and SQL can be used.

To install EventTracker 21 day trial – Standard/Collection Point, please follow the steps given below.

1. Double-click the executable file.

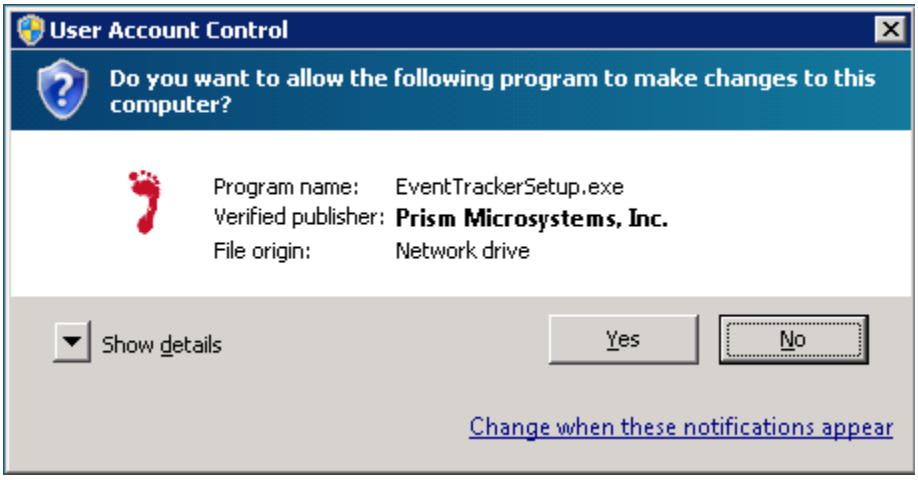

User Account Control
Do you want to allow the following program to make changes to this computer?
Program name: EventTrackerSetup.exe
Verified publisher: Prism Microsystems, Inc.
File origin: Network drive
Show details
Yes
No
Change when these notifications appear

Figure 114

2. Click the **Yes** button.

   EventTracker Pre-Install Check window displays.

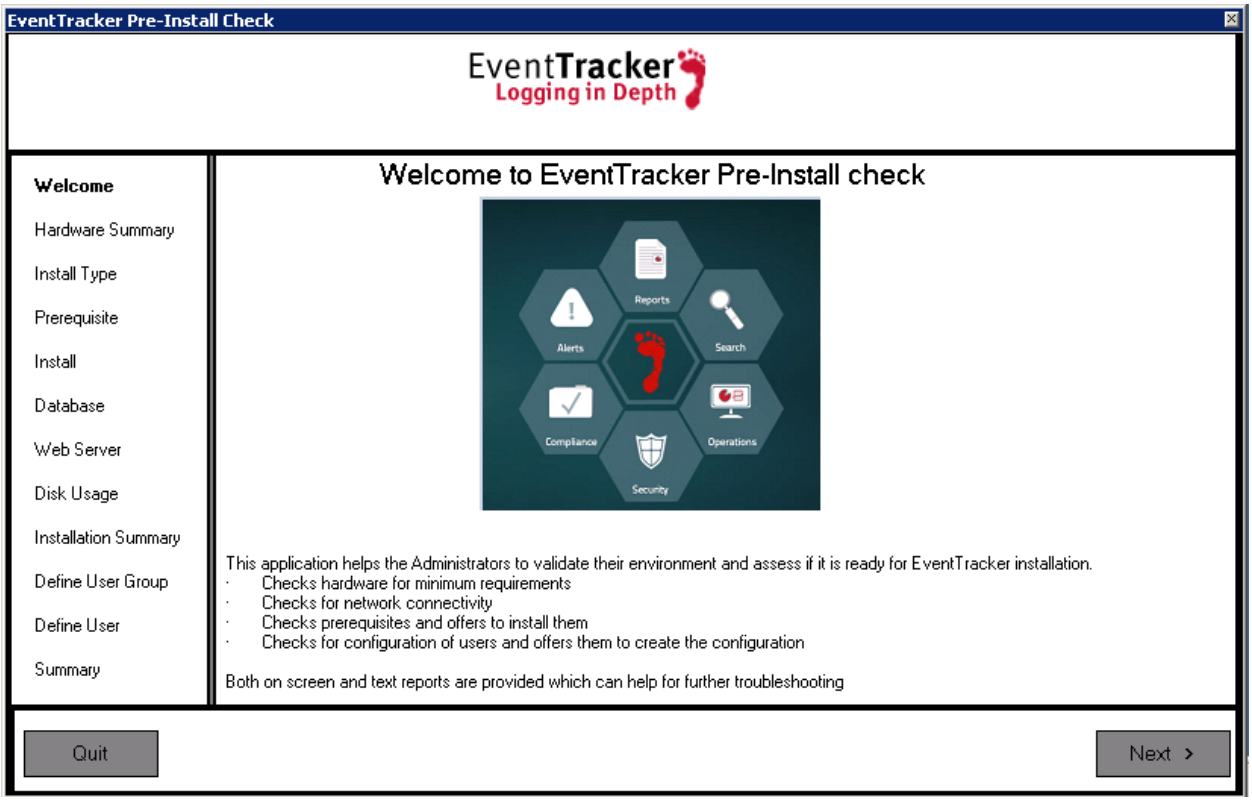


Figure 115

3. Click the **Next >** button.

   Hardware Summary pane displays.

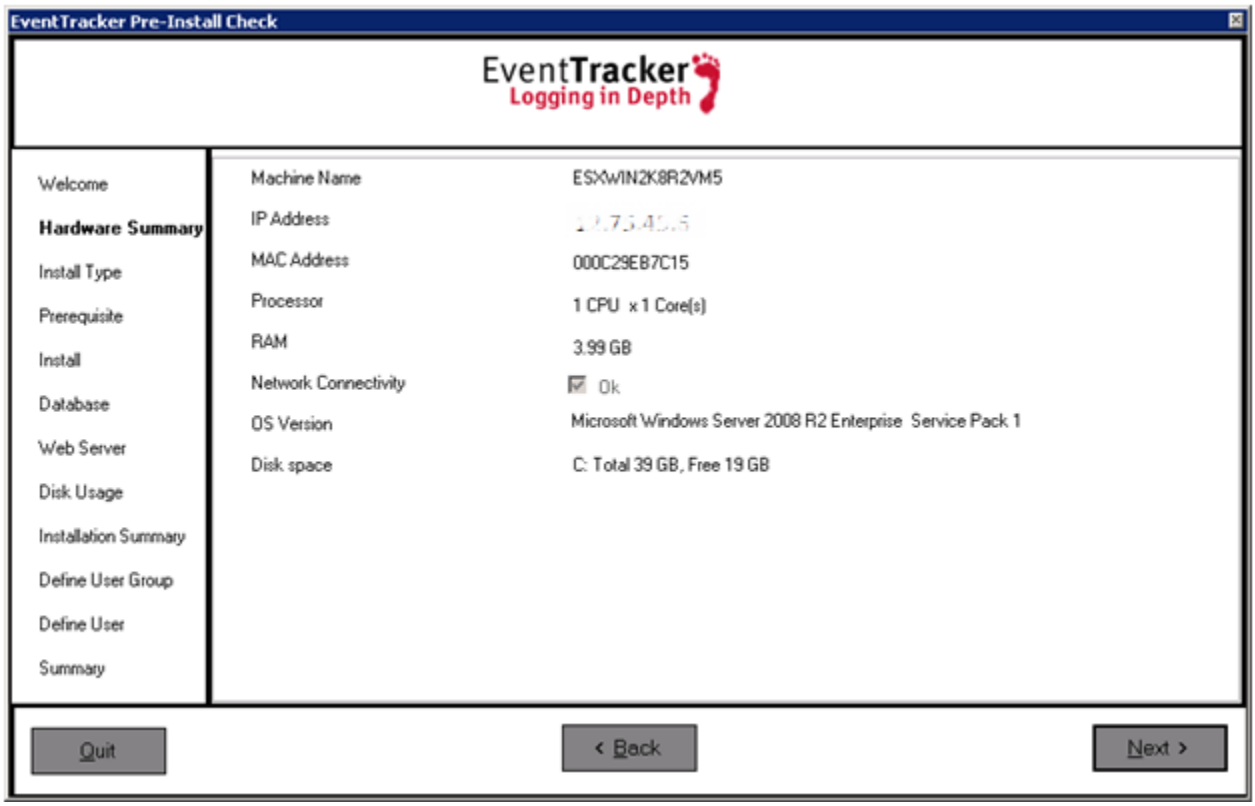


Figure 116

4. Select **Standard/Collection Point** option, and then select the **Next >** button.

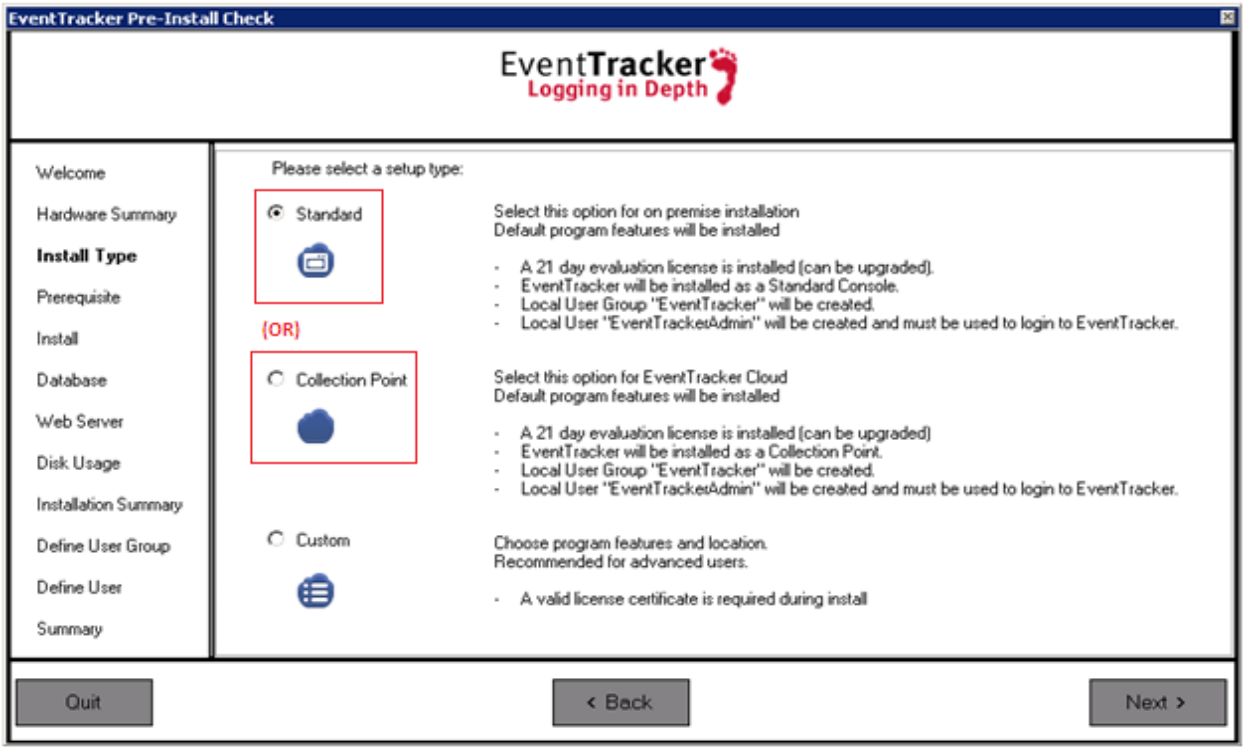

EventTracker Pre-Install Check
EventTracker
Logging in Depth
Welcome
Hardware Summary
Install Type
Prerequisite
Install
Database
Web Server
Disk Usage
Installation Summary
Define User Group
Define User
Summary
Please select a setup type:
Standard
Select this option for on premise installation
Default program features will be installed
- A 21 day evaluation license is installed (can be upgraded).
- EventTracker will be installed as a Standard Console.
- Local User Group "EventTracker" will be created.
- Local User "EventTrackerAdmin" will be created and must be used to login to EventTracker.
(OR)
Collection Point
Select this option for EventTracker Cloud
Default program features will be installed
- A 21 day evaluation license is installed (can be upgraded)
- EventTracker will be installed as a Collection Point.
- Local User Group "EventTracker" will be created.
- Local User "EventTrackerAdmin" will be created and must be used to login to EventTracker.
Custom
Choose program features and location.
Recommended for advanced users.
- A valid license certificate is required during install
Quit
< Back
Next >

Figure 117

Prerequisites page displays.

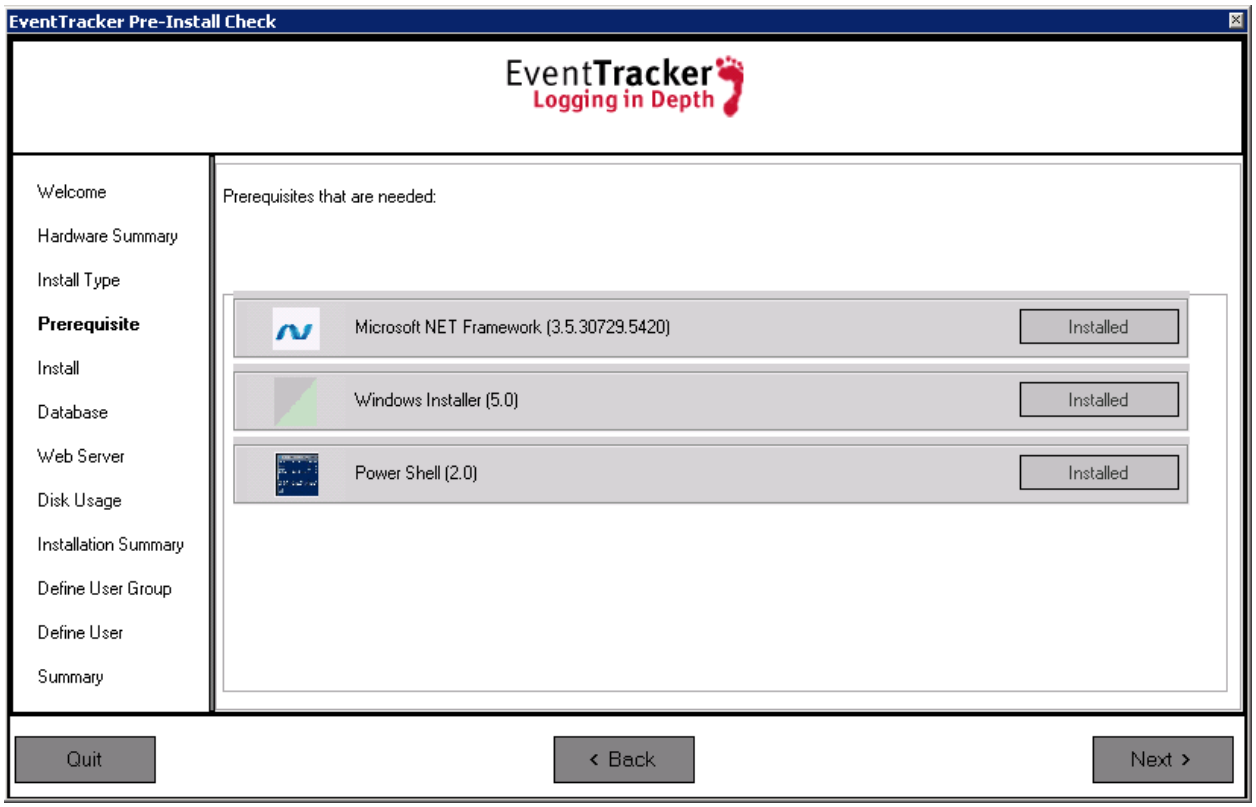


Figure 118

If prerequisites are not installed, please refer Figure 61- Figure 64 to install all the prerequisites mentioned.

5. Click the **Next >** button.

   If all the prerequisites are installed, then Database page displays.

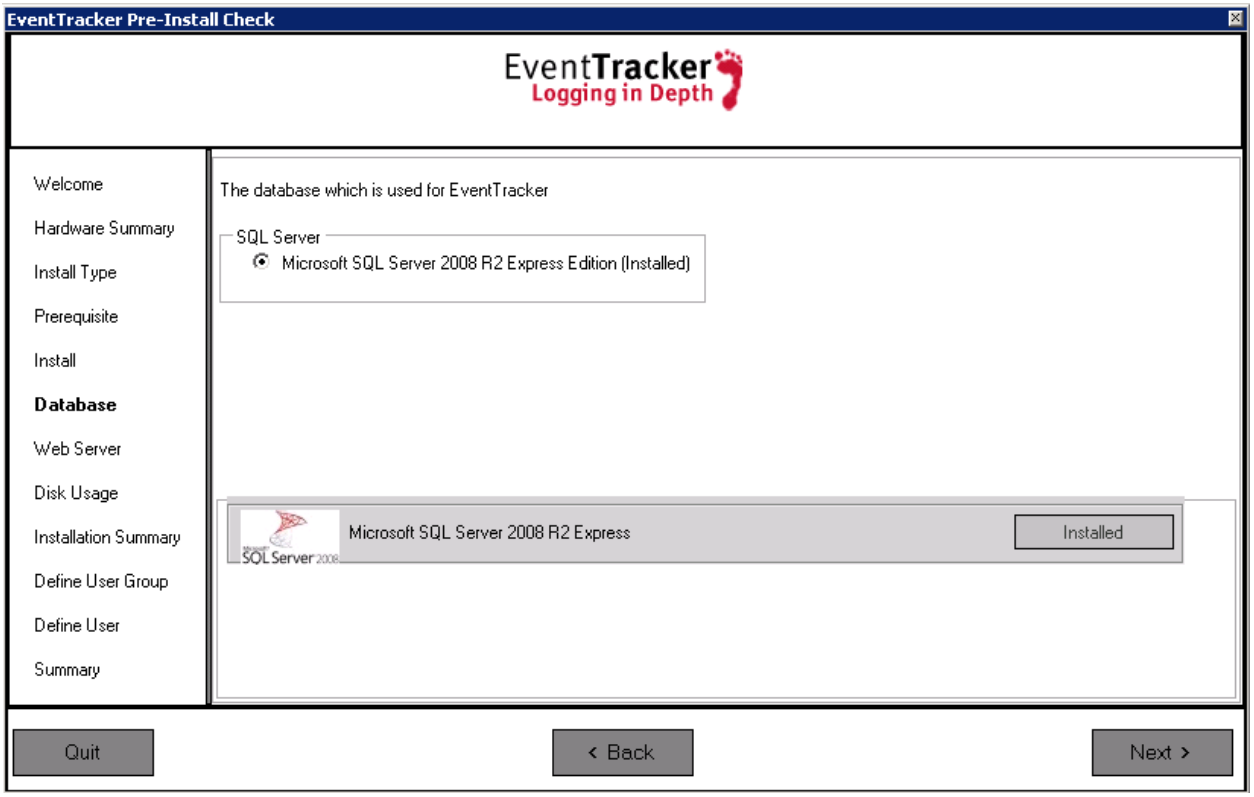


Figure 119

If MS SQL Server Express is not installed, please refer Figure 65 – Figure 69 for detail instructions.

6. Click the **Next >** button.

   IIS Web Server page displays.

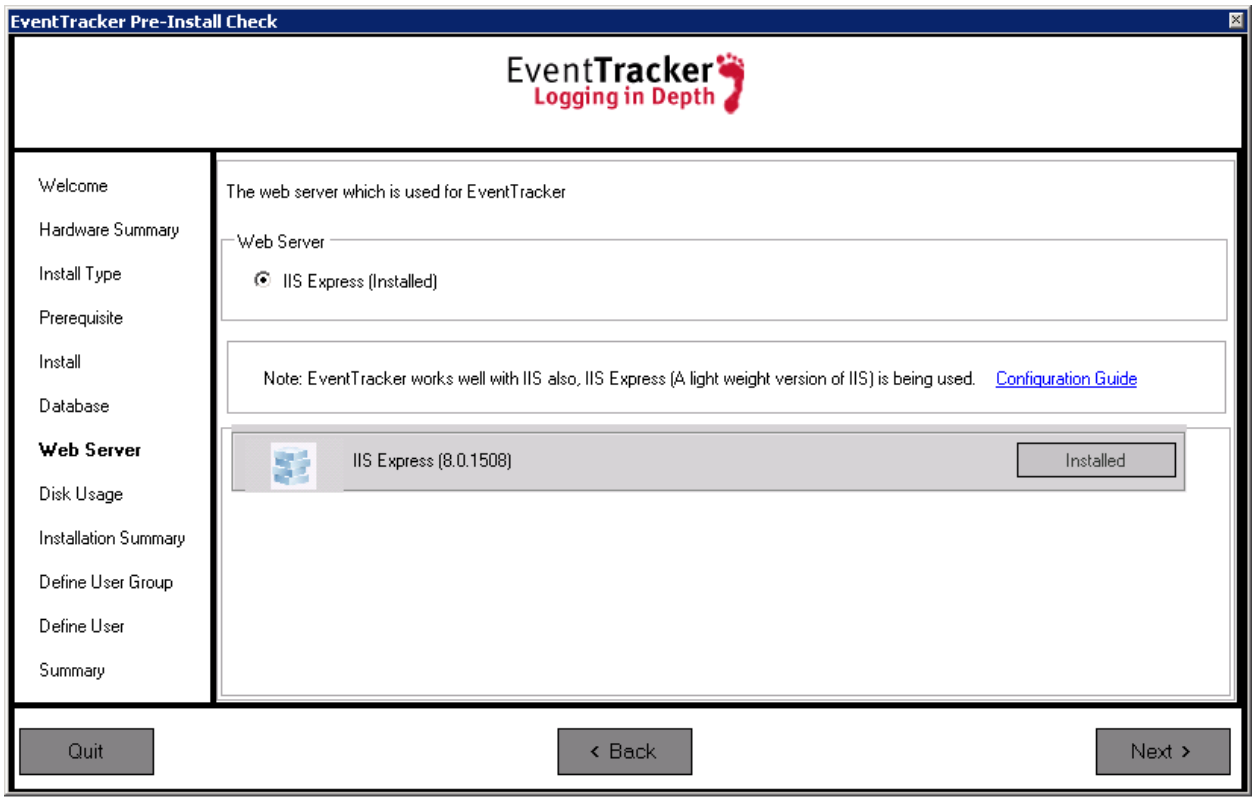


Figure 120

If IIS Express is installed, then Define User page displays if EventTrackerAdmin user is not created otherwise Summary page displays.

If IIS Express is not installed, please refer Figure 70 - Figure 73 for detail instructions.

7. Enter **EventTrackerAdmin** credentials, and then click the **Next >** button.

NOTE:

It will be displayed only if there are two instances of SQL running or some pre-requisites are missing.

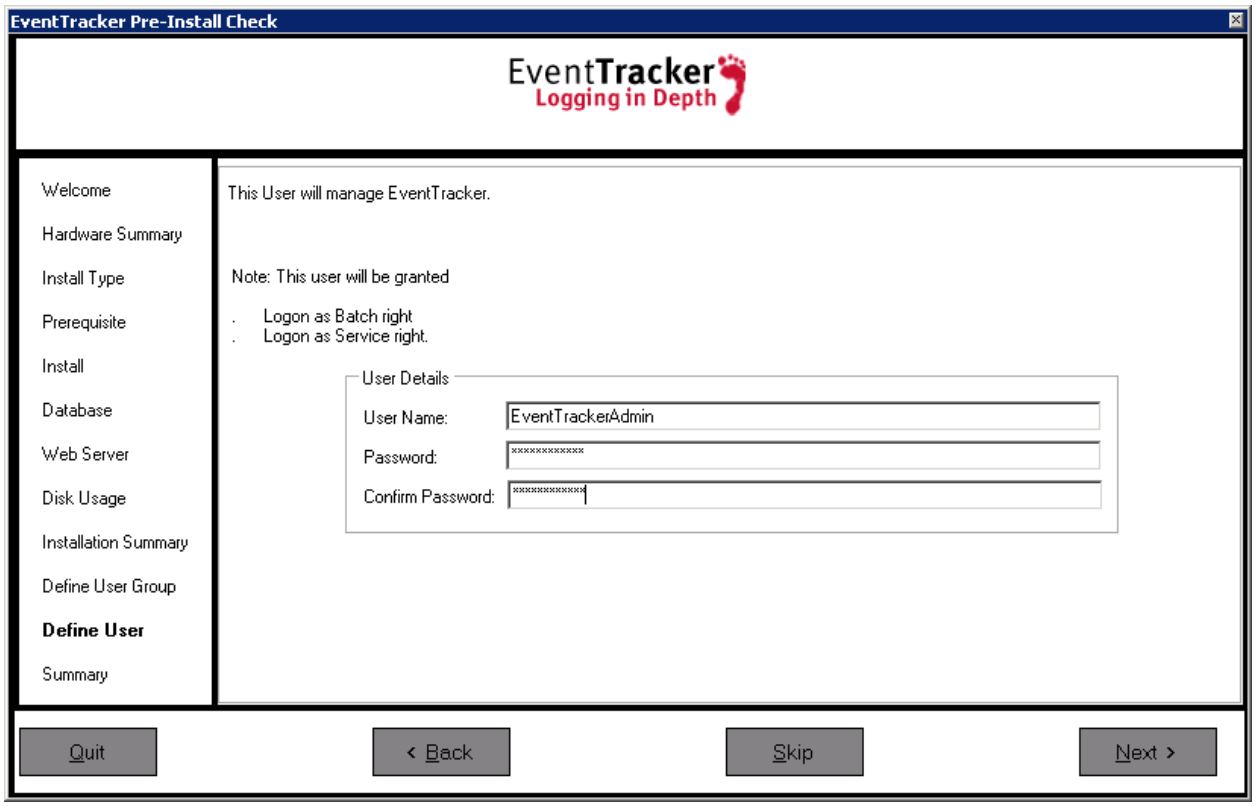


Figure 121

Summary page displays.

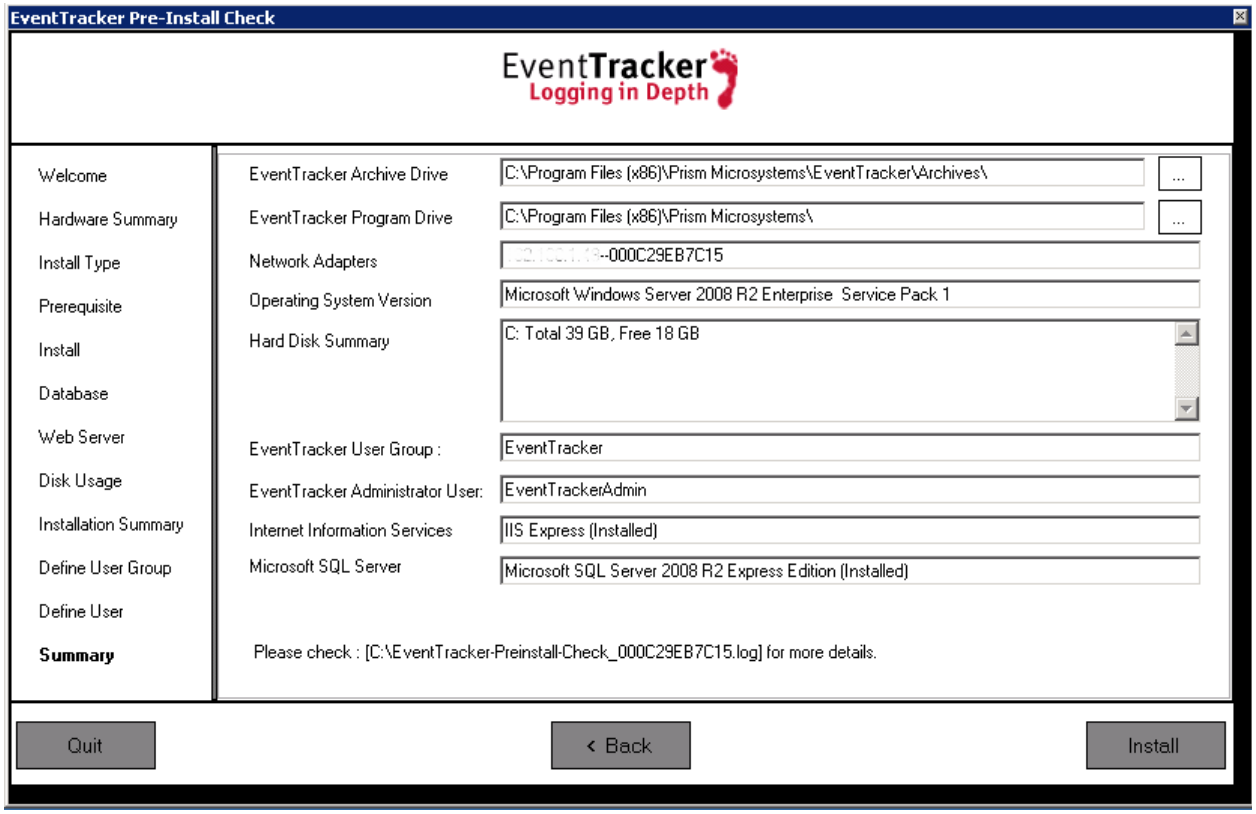


Figure 122

Welcome page displays.

EventTracker 7.5
7.5
EventTracker
Logging In Depth
Welcome to EventTracker Setup Program.
This setup program will install EventTracker on your computer. To continue, click Next.
WARNING: This program is protected by copyright law and international treaties.
Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.
© Copyright 1999-2014 Prism Microsystems, Inc.
< Back
Next >
Cancel

Figure 123

8. Click the **Next >** button.

   License Agreement page displays.

9. Select **I accept the terms in the license agreement** option, and then select the **Next >** button.

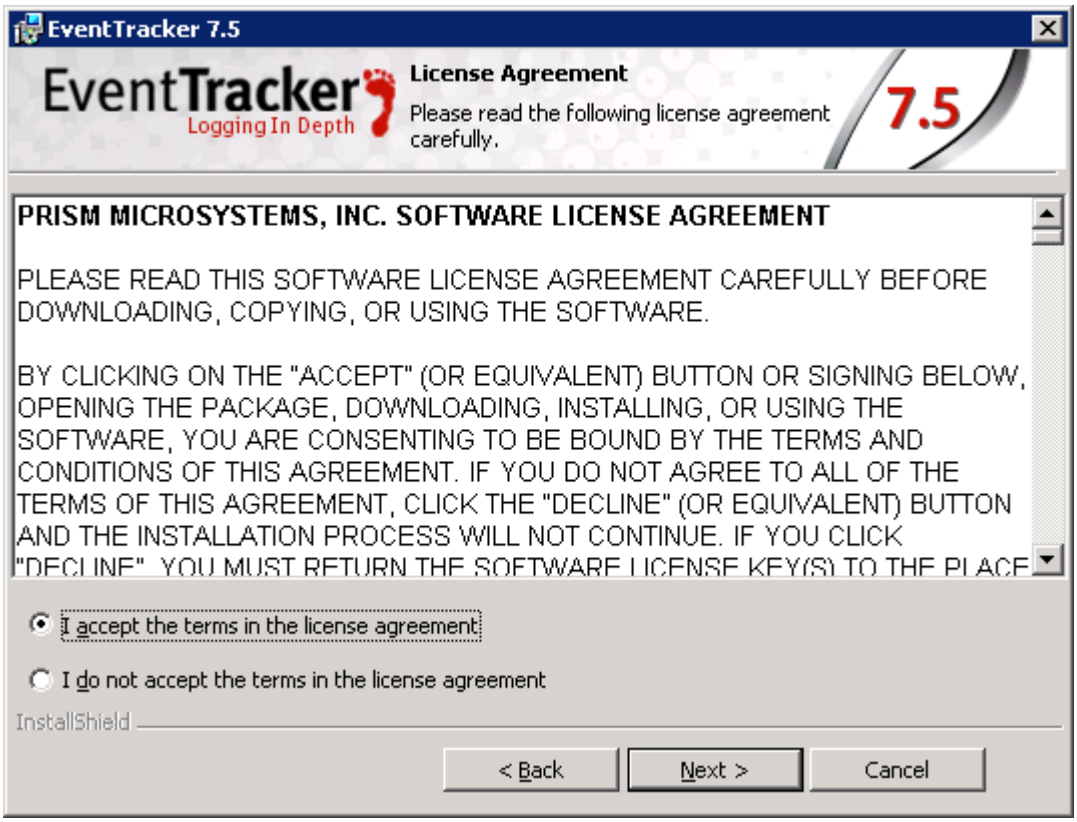

EventTracker 7.5
EventTracker
Logging In Depth
License Agreement
Please read the following license agreement carefully.
7.5
PRISM MICROSYSTEMS, INC. SOFTWARE LICENSE AGREEMENT
PLEASE READ THIS SOFTWARE LICENSE AGREEMENT CAREFULLY BEFORE DOWNLOADING, COPYING, OR USING THE SOFTWARE.
BY CLICKING ON THE "ACCEPT" (OR EQUIVALENT) BUTTON OR SIGNING BELOW, OPENING THE PACKAGE, DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU ARE CONSENTING TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE "DECLINE" (OR EQUIVALENT) BUTTON AND THE INSTALLATION PROCESS WILL NOT CONTINUE. IF YOU CLICK
I accept the terms in the license agreement
I do not accept the terms in the license agreement
InstallShield
< Back
Next >
Cancel

Figure 124

If **Standard** option is selected earlier, then Install Default Remedial action displays. Please refer Figure 127.

If **Collection Point** option is selected earlier, then Configure Collection Point site page displays.

10. Enter the **Collection Point** name and then click the **Next >** button.

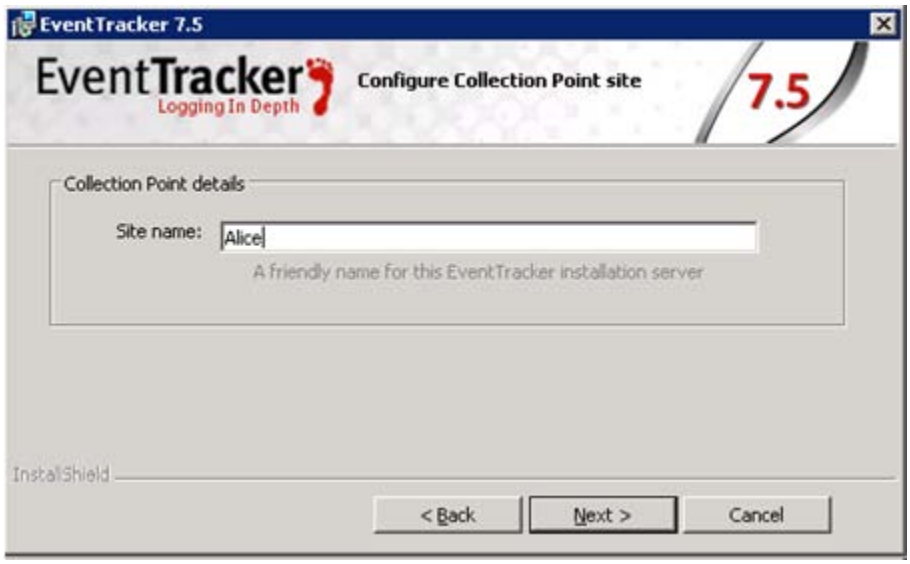


Figure 125

Configure Collection Master page displays.

11. Enter **Collection Master:** name or IP address, and then click the **Next >** button.

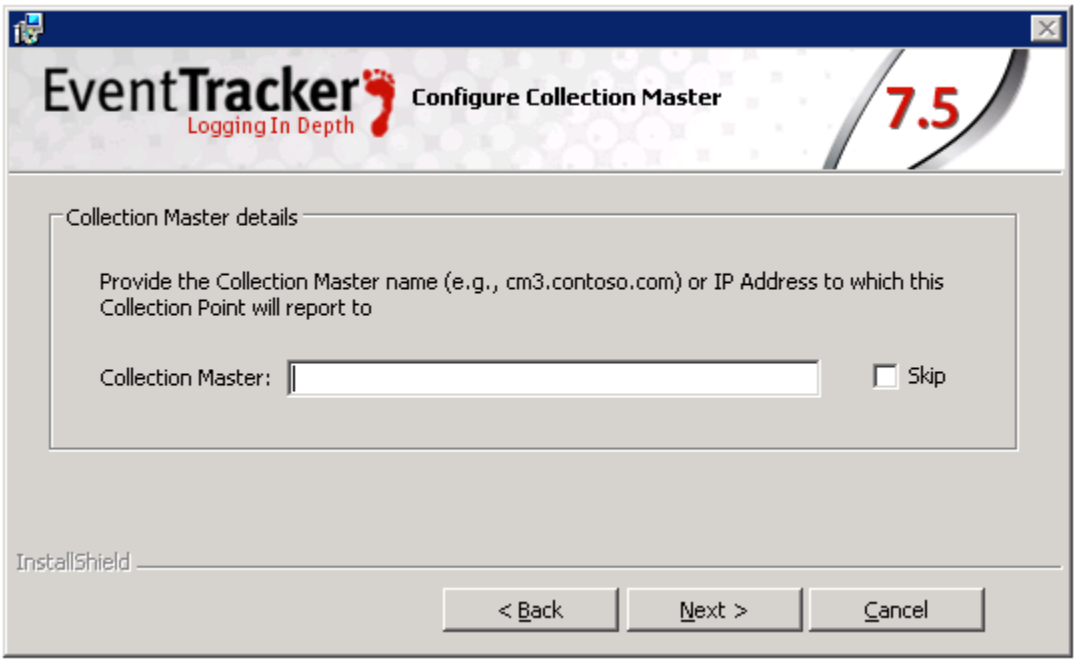


Figure 126

Ready to install the program page displays.

12. Select **Install default Remedial Action EXEs on this machine** option, and then select the **Install** button.

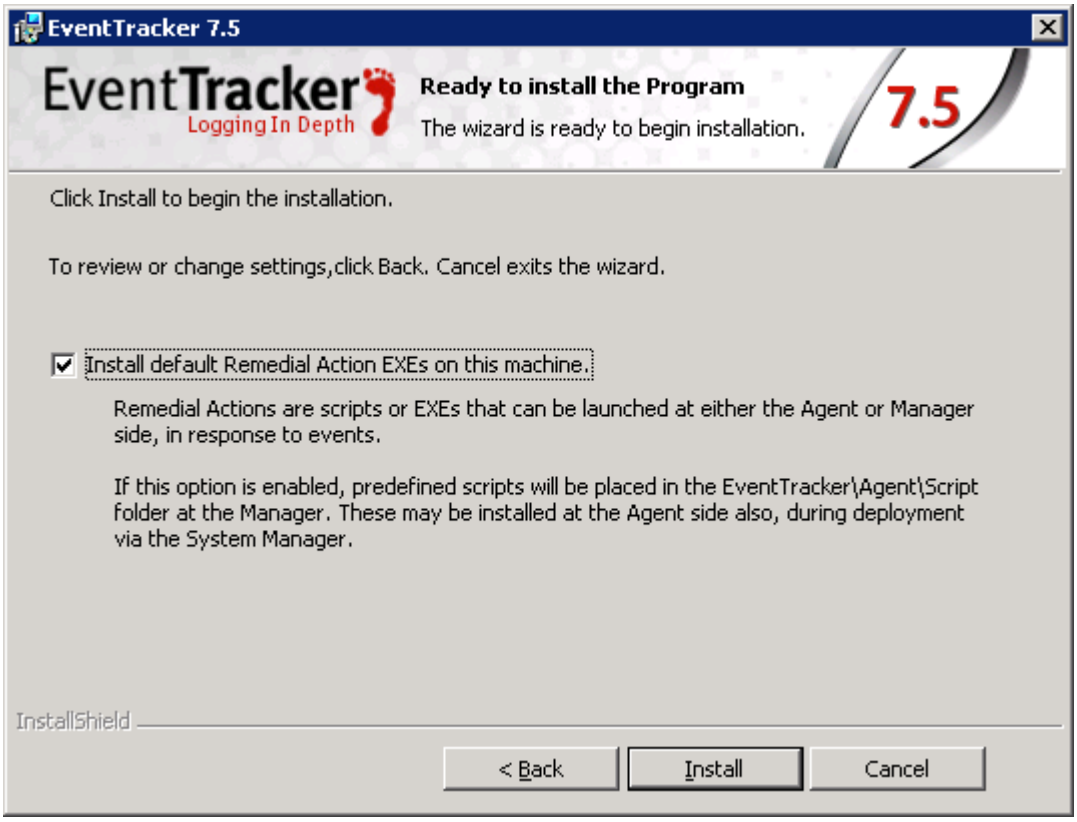

EventTracker 7.5
EventTracker
Logging In Depth
Ready to install the Program
The wizard is ready to begin installation.
7.5
Click Install to begin the installation.
To review or change settings,click Back. Cancel exits the wizard.
Install default Remedial Action EXEs on this machine.
Remedial Actions are scripts or EXEs that can be launched at either the Agent or Manager side, in response to events.
If this option is enabled, predefined scripts will be placed in the EventTracker\Agent\Script folder at the Manager. These may be installed at the Agent side also, during deployment via the System Manager.
InstallShield
< Back
Install
Cancel

Figure 127

A successful message displays.

EventTracker 7.5
EventTracker
Logging In Depth
EventTracker installation is finished
7.5
Options
Import existing event log entries.
Event logs from this machine will be imported.
Add a shortcut to the desktop.
Add EventTracker Control Panel to the desktop.
Add EventTracker Diagnostics as a startup program.
Helps to notify problems about EventTracker if any.
The InstallShield Wizard has successfully installed EventTracker. Click Finish to exit the wizard.
InstallShield
< Back
Finish
Cancel

Figure 128

13. Click the **Finish** button.

    EventTracker :: Configuration window displays.

14. Enter valid user credentials and then click the **OK** button.

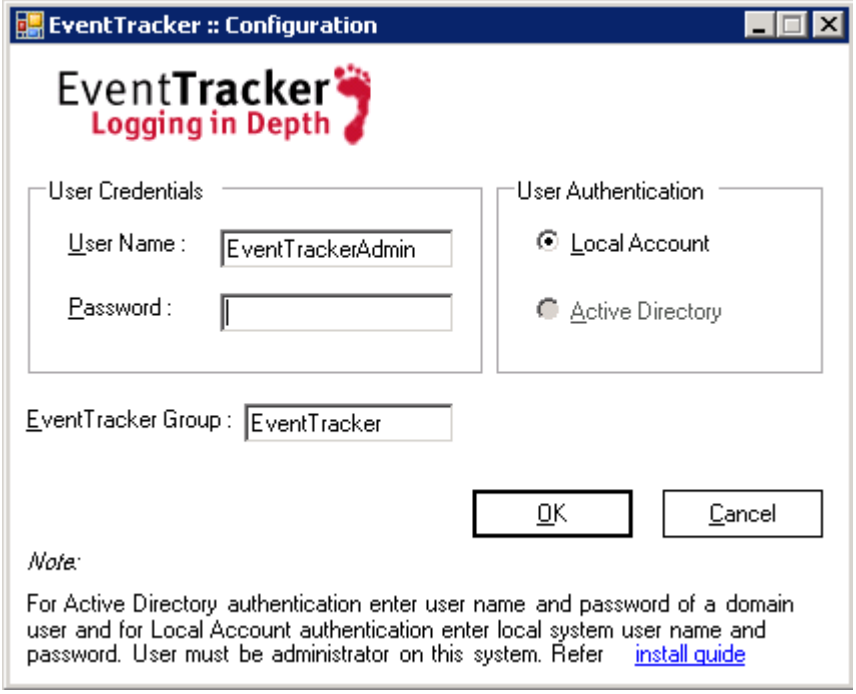


Figure 129

NOTE: After logging into EventTracker Enterprise, some of the components are not available as it is a trial version.

In **Collection Point** installation, components like **Trap Tracker, Reports** etc are omitted.

Procedure to install EventTracker Manager for v7.5.29 and below versions

If you are using EventTracker for the first time, launch the executable program etwrel75.exe and then proceed. If you are a second time user, please uninstall the previous version of EventTracker and then proceed. The detail procedure to uninstall EventTracker is mentioned in Uninstall EventTracker.

The detail procedure to install EventTracker is given below.

1. Double-click **etwrel.exe.**

   Setup prepares the InstallShield[R] Wizard for installation.

Figure 130

EventTracker checks for all the prerequisites.

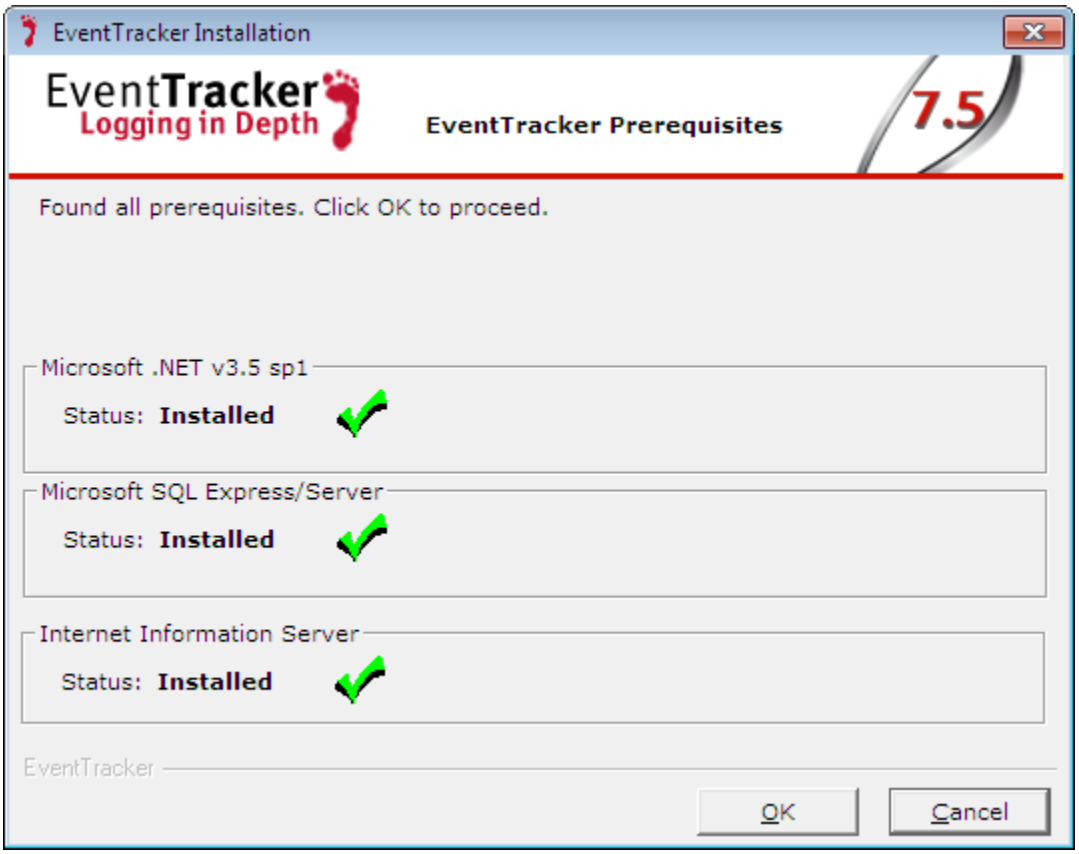


Figure 131

NOTE:

If there are two instances of MS SQL running or some prerequisites are missing, then the EventTracker Prerequisites will be displayed otherwise it will not be displayed.

2. Click the **OK** to proceed with installation.

3. In case of multiple SQL instances, select the appropriate instance name from **Instance name** dropdown, and then click the **OK** button.

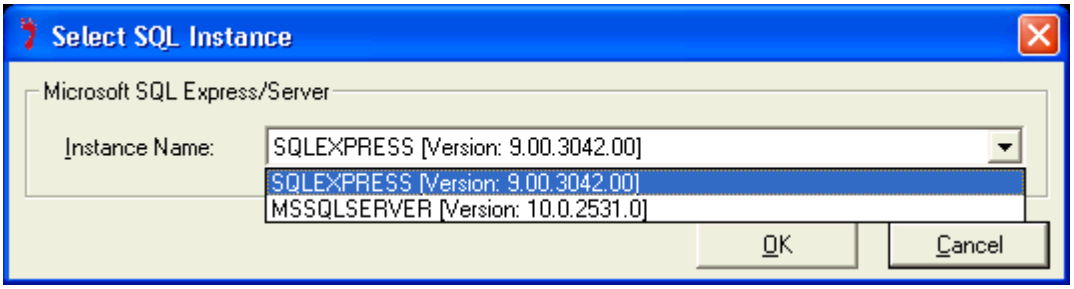


Figure 132

☐

NOTE:
If default instance of SQLEXPRESS is present in the system, then EventTracker won't

prompt for this screen. If the selected SQL Instance is not running then EventTracker Installation wizard will display a message.

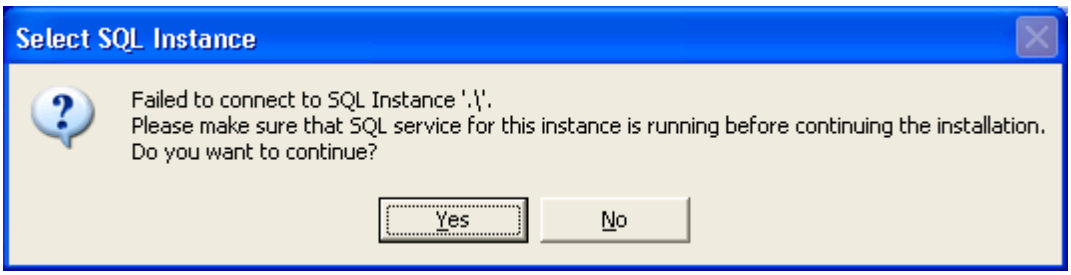

Select SQL Instance
Failed to connect to SQL Instance '.\'.
Please make sure that SQL service for this instance is running before continuing the installation.
Do you want to continue?
Yes
No

Figure 133

4. Click **Yes** to continue.

   (OR)

   Click **No** to abort the installation process, and then click the **Finish** button.

   If the mandatory components are found to be installed, InstallShield[R] Wizard displays the EventTracker dialog box.

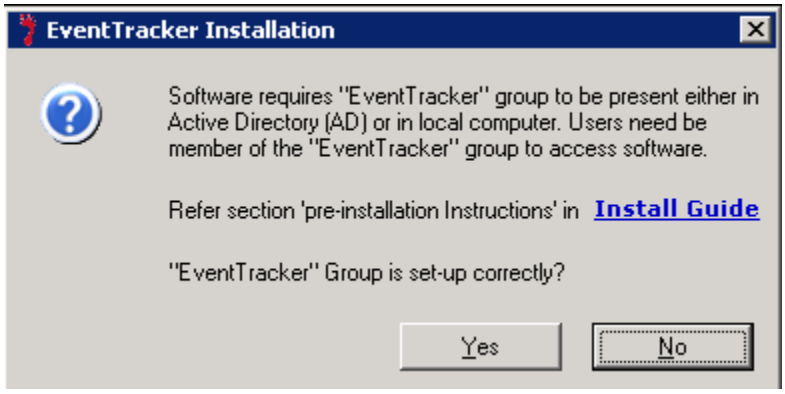

EventTracker Installation
Software requires "EventTracker" group to be present either in Active Directory (AD) or in local computer. Users need be member of the "EventTracker" group to access software.
Refer section 'pre-installation Instructions' in Install Guide
"EventTracker" Group is set-up correctly?
Yes
No

Figure 134

NOTE:
If another user who does not have SQL sysadmin privilege has logged in to the system and tries to install EventTracker, then an error message is displayed. Please refer User Permission on SQL Server for detail instructions.

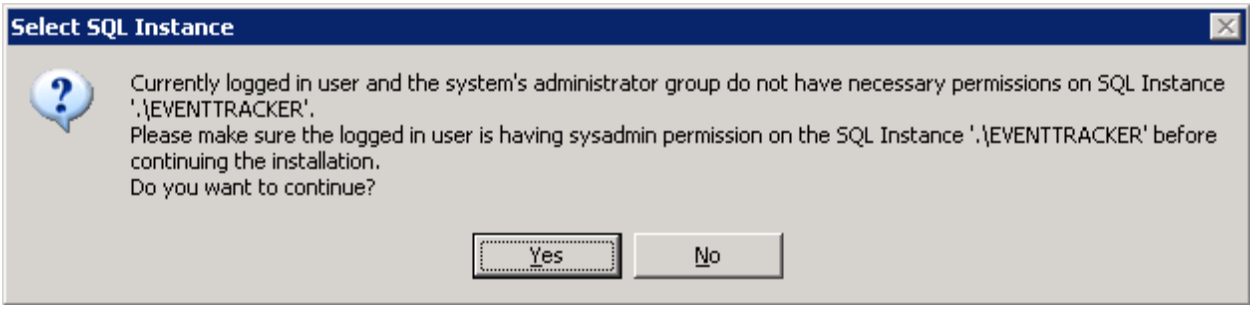

Select SQL Instance
Currently logged in user and the system's administrator group do not have necessary permissions on SQL Instance '.\EVENTTRACKER'.
Please make sure the logged in user is having sysadmin permission on the SQL Instance '.\EVENTTRACKER' before continuing the installation.
Do you want to continue?
Yes
No

Figure 135

5. Click **Yes** to continue, had you created Local / Active Directory user group and added users to that group prior to this installation attempt.

   InstallShield[R] Wizard displays the **Welcome** screen.

EventTracker 7.5
EventTracker
Logging in Depth
7.5
Welcome to EventTracker Setup Program.
This setup program will install EventTracker on your computer. To continue, click Next.
WARNING: This program is protected by copyright law and international treaties.
Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.
© Copyright 1999-2013 Prism Microsystems, Inc.
< Back
Next >
Cancel

Figure 136

(OR)

Click **No** to abort the installation process, and then click the **Finish** button.

NOTE:

If the required components are not installed or found to be missing, InstallShield[R] Wizard

displays the EventTracker Prerequisites dialog box with appropriate message.

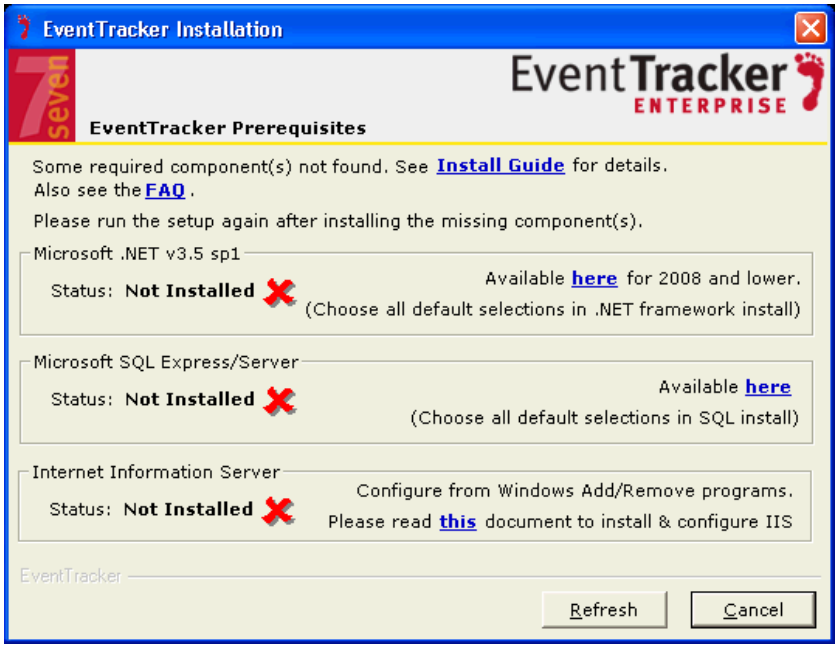

EventTracker Installation
EventTracker ENTERPRISE
EventTracker Prerequisites
Some required component(s) not found. See Install Guide for details.
Also see the FAQ.
Please run the setup again after installing the missing component(s).
Microsoft .NET v3.5 sp1
Status: Not Installed
Available here for 2008 and lower.
(Choose all default selections in .NET framework install)
Microsoft SQL Express/Server
Status: Not Installed
Available here
(Choose all default selections in SQL install)
Internet Information Server
Status: Not Installed
Configure from Windows Add/Remove programs.
Please read this document to install & configure IIS
EventTracker
Refresh
Cancel

Figure 137

Click the **Cancel** button, and then click the **Finish** button.

InstallShield[R] Wizard safely exits the installation process.

After installing the mandatory components, start installing EventTracker Enterprise afresh.

(OR)

Keep the installation wizard open, install the prerequisites, and then click the **Refresh** button.

Click the **OK** button to continue with the installation process.

6. Click **Next>**.

   InstallShield[R] Wizard displays the **License Agreement** screen.

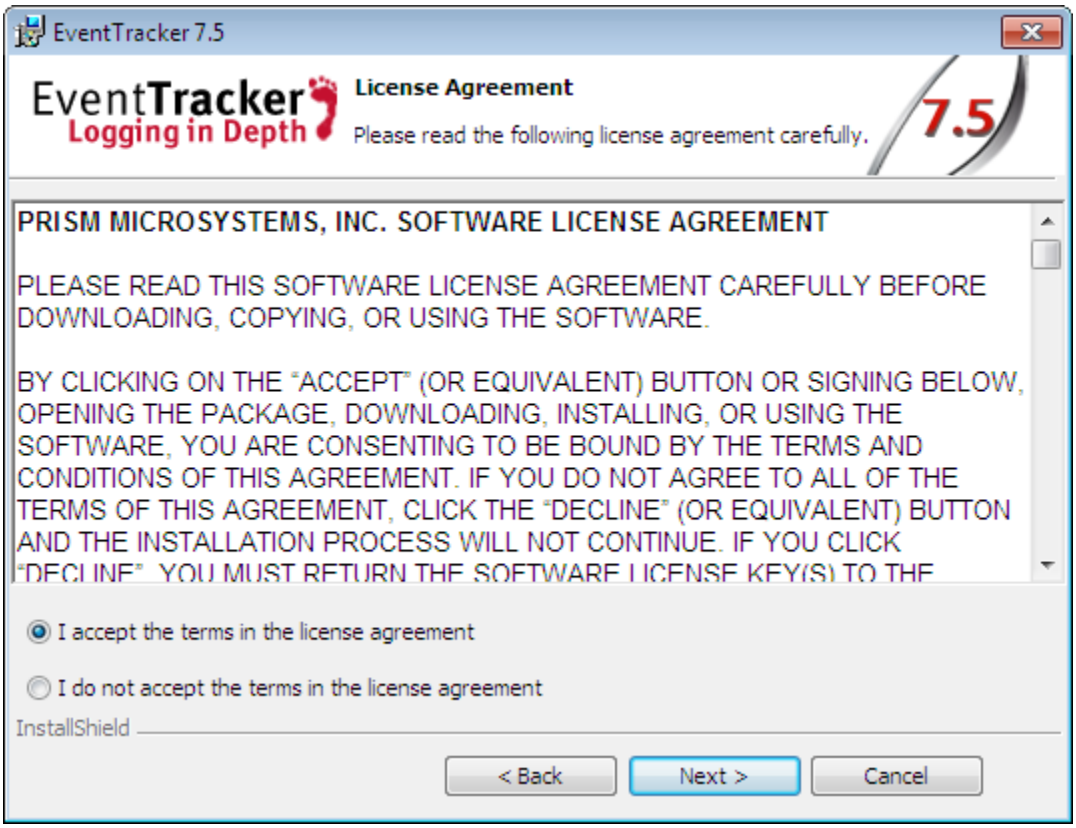

EventTracker 7.5
EventTracker
Logging in Depth
License Agreement
Please read the following license agreement carefully.
7.5
PRISM MICROSYSTEMS, INC. SOFTWARE LICENSE AGREEMENT
PLEASE READ THIS SOFTWARE LICENSE AGREEMENT CAREFULLY BEFORE DOWNLOADING, COPYING, OR USING THE SOFTWARE.
BY CLICKING ON THE "ACCEPT" (OR EQUIVALENT) BUTTON OR SIGNING BELOW, OPENING THE PACKAGE, DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU ARE CONSENTING TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE "DECLINE" (OR EQUIVALENT) BUTTON AND THE INSTALLATION PROCESS WILL NOT CONTINUE. IF YOU CLICK
I accept the terms in the license agreement
I do not accept the terms in the license agreement
InstallShield
< Back
Next >
Cancel

Figure 138

7. Read the license agreement, and then click '**I accept the terms in the license agreement**' option to accept the terms and condition.
8. Select the **Next >** button.

   InstallShield[R] Wizard prompts to provide the path of the certificate file.

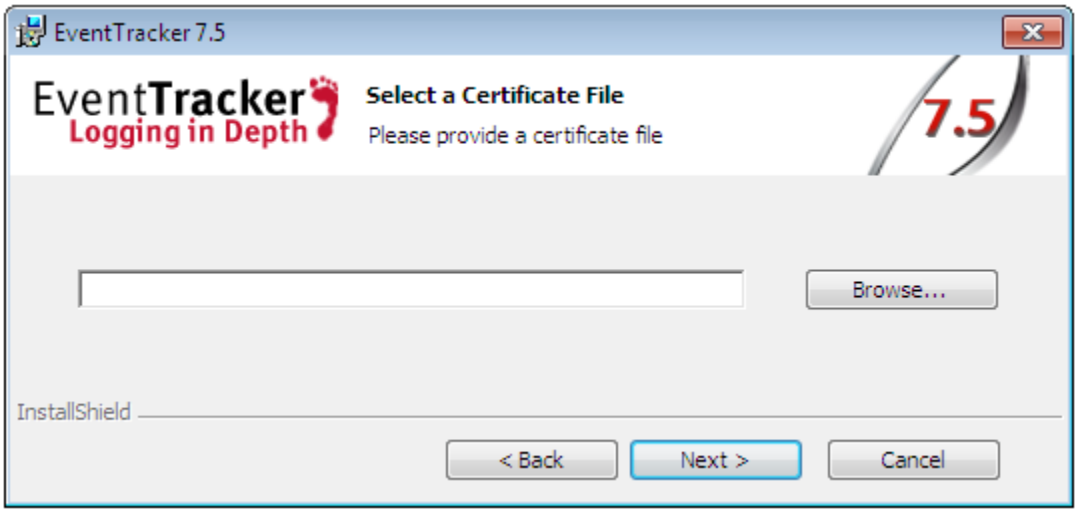


Figure 139

9. Click the **Browse** button.

   InstallShield[R] Wizard displays the **Select File** window.

10. Go to the appropriate folder, and then select the file.

11. Click **Open**.

    InstallShield[R] Wizard updates the folder path.

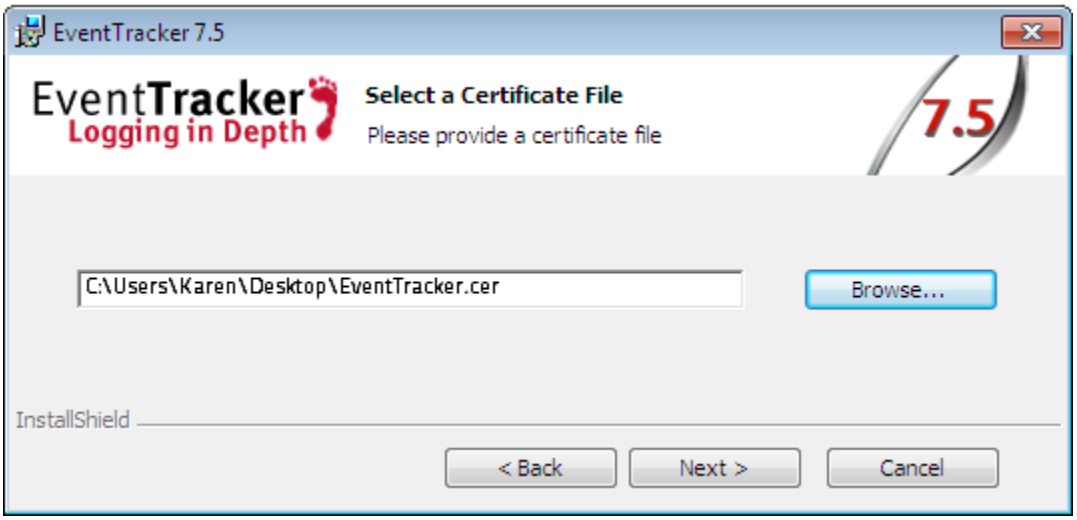


Figure 140

12. Click **Next >**.

    InstallShield Wizard displays the **Select Components** screen.

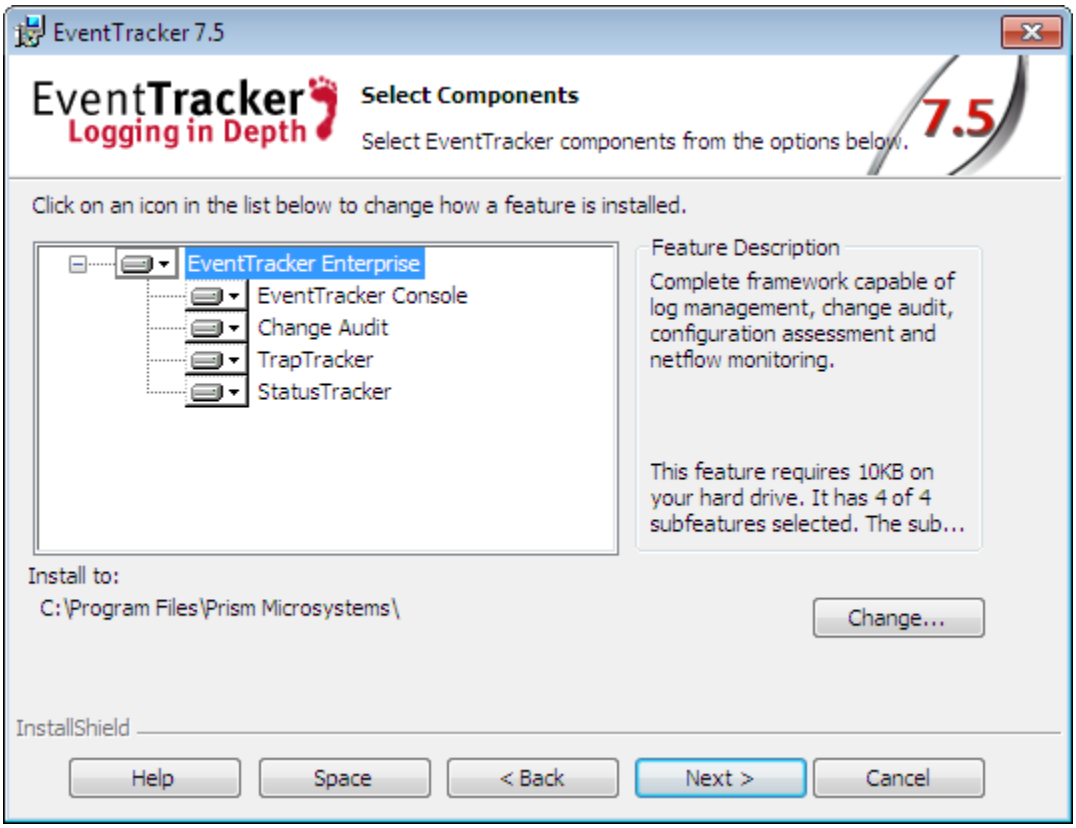
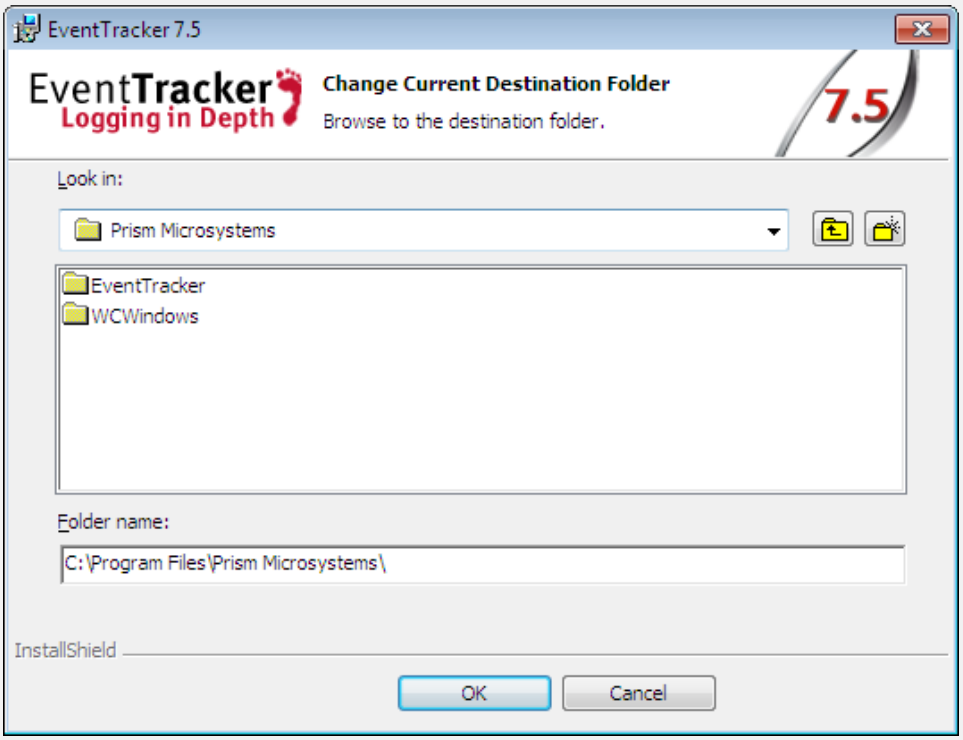
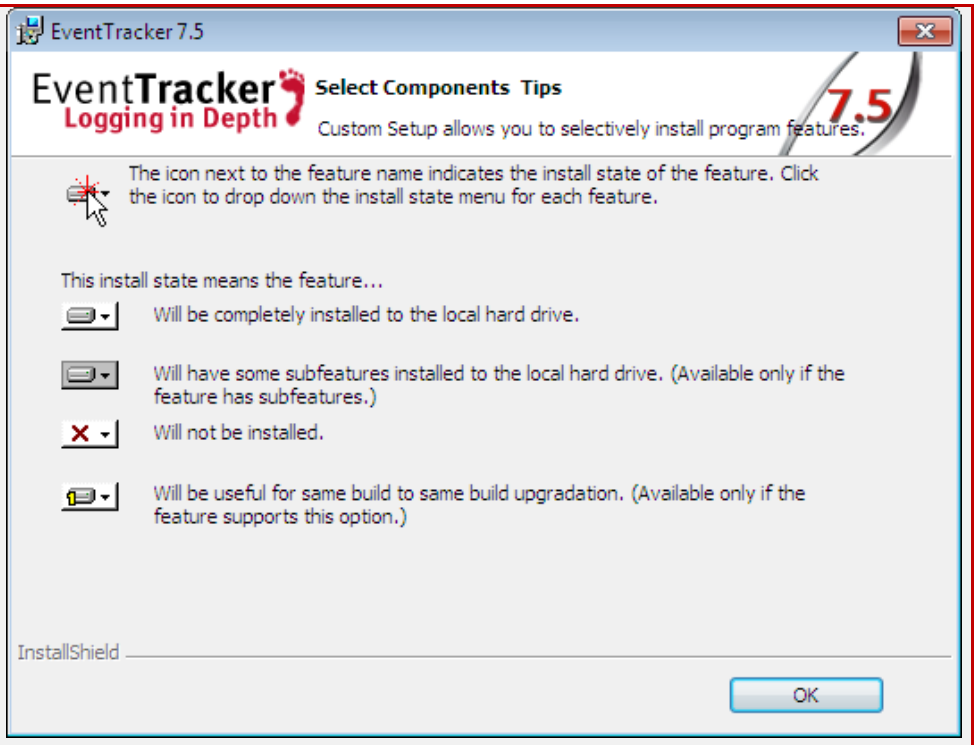


Figure 141

EventTracker Components	Description
EventTracker Console	Select this option to install manager console on the target computer.
Change Audit	Optional component. Installing this component enables you to monitor and manage change over the enterprise. Agent component will also be installed along with the Manager Console. You can also deploy agent to the monitored computers using System Manager after installing the Manager Console.
Trap Tracker	Optional component. Installing this component enables you to monitor and manage traps sent by SNMP compliant devices.

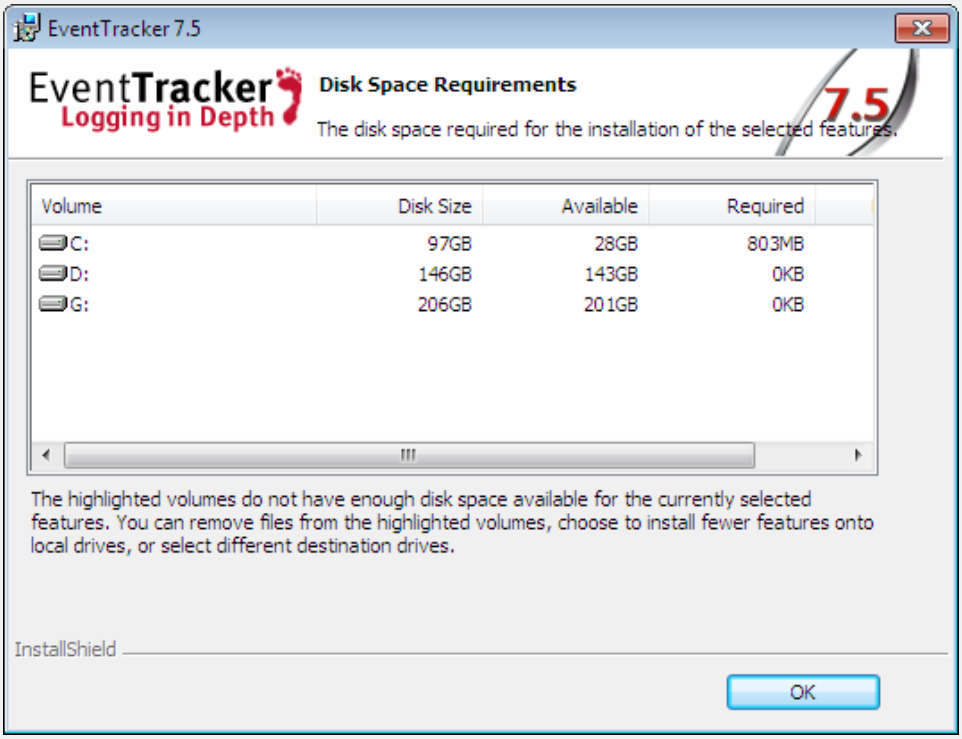
Status Tracker	Optional component. Installing this component enable you to monitor and manage TCP/IP networks, Web sites, applications, and ports in mission critical environment.

Click	To
Change...	Select different destination folder to install EventTracker. 
Help	View **Select Component** conventions.


EventTracker 7.5
EventTracker
Logging in Depth
Select Components Tips
Custom Setup allows you to selectively install program features.
7.5
The icon next to the feature name indicates the install state of the feature. Click the icon to drop down the install state menu for each feature.
This install state means the feature...
Will be completely installed to the local hard drive.
Will have some subfeatures installed to the local hard drive. (Available only if the feature has subfeatures.)
Will not be installed.
Will be useful for same build to same build upgradation. (Available only if the feature supports this option.)
InstallShield
OK

Space

Check the disk space available in the target computer.



13. Click **Next** >.

InstallShield[R] Wizard displays the **Select EventTracker Console Type** screen.

Standard Console:

Best for flat network topologies where all monitored nodes report directly to one (or redundant) EventTracker Console.

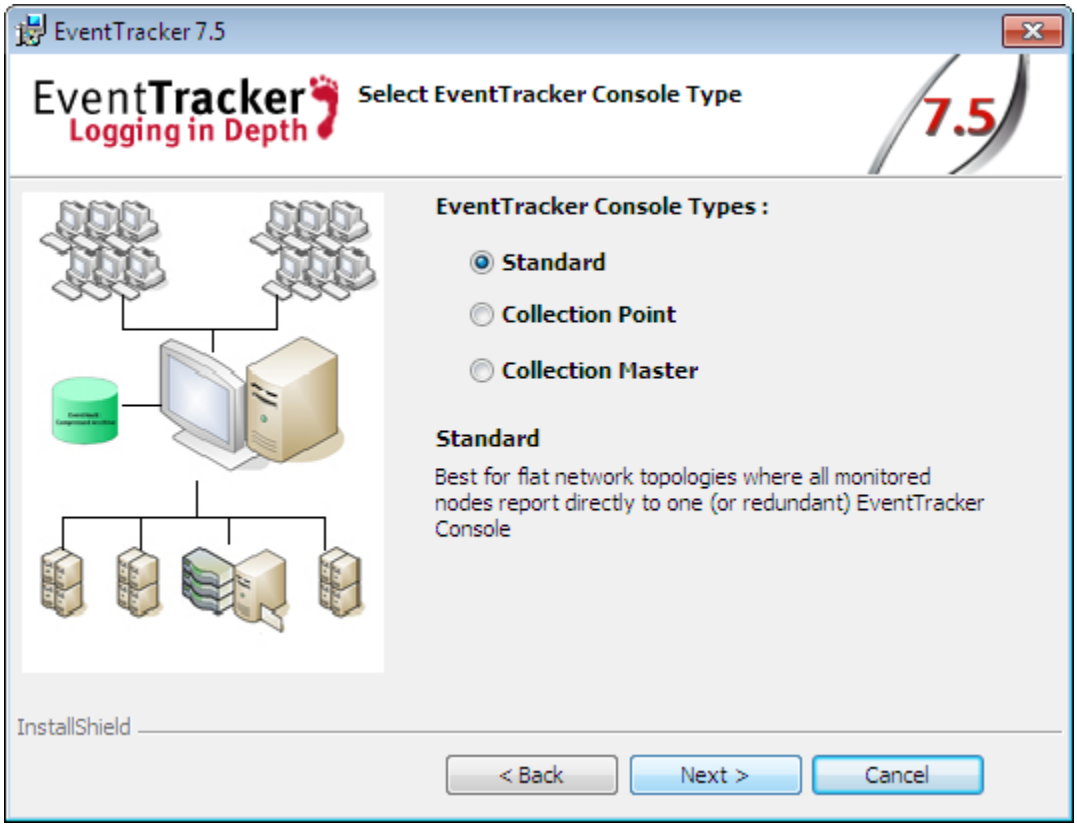


Figure 142

Collection point:

Used in hierarchical network topologies where monitored nodes report to a local EventTracker Console which in turn replicates its event log archive to a Collection Master.

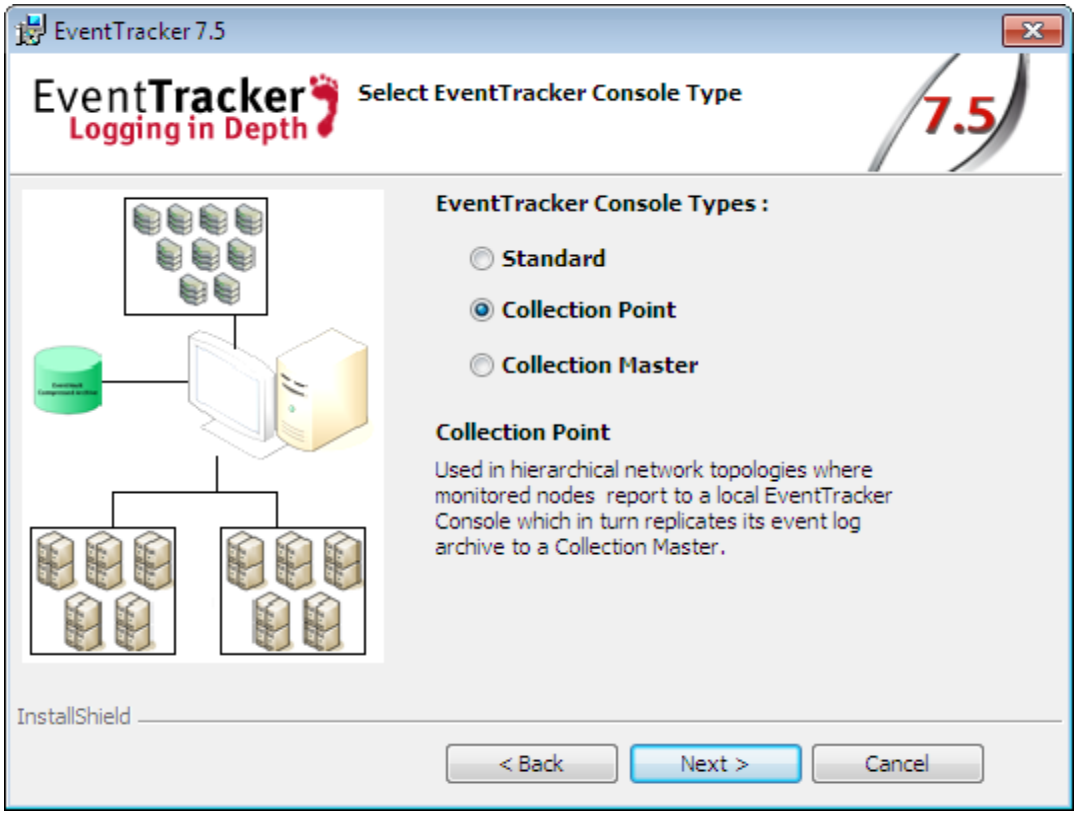


Figure 143

a) Select the console type as **Collection Point**, and then click **Next >**.

InstallShield[R] Wizard displays **Site or group name** screen.

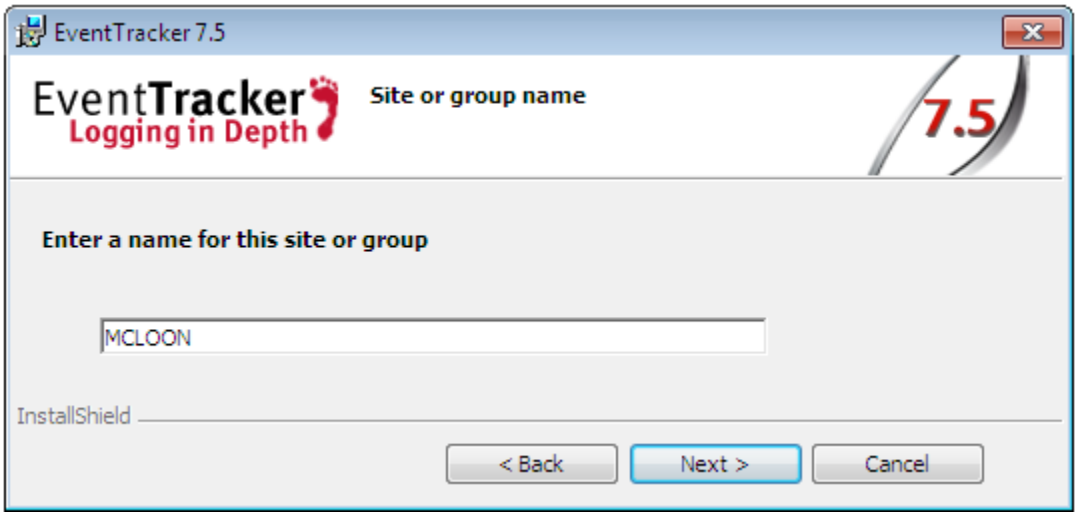


Figure 144

b) Type an appropriate group/site name for the **Collection Point**, and then click **Next** >.

NOTE:

Some special characters are not allowed while providing site/group name. InstallShield[R] Wizard will display a pop-up window if site or group name is provided with such special characters.

Figure 145

Collection Master:

Used in hierarchical network topologies where collection points replicate their event log archives to a Collection Master.

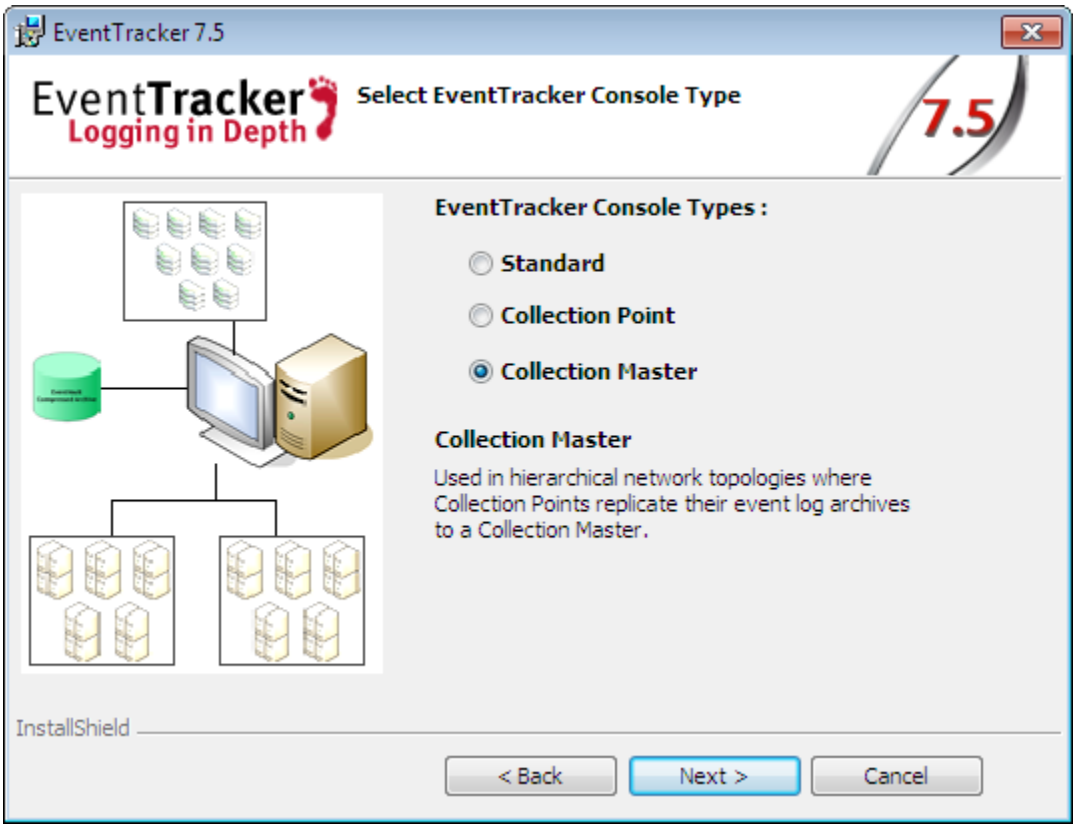


Figure 146

14. Select a console type, and then click **Next >**.

    If you have selected **Change Audit** component**,** then InstallShield[R] Wizard displays **Change Audit SnapShot** dialog box.

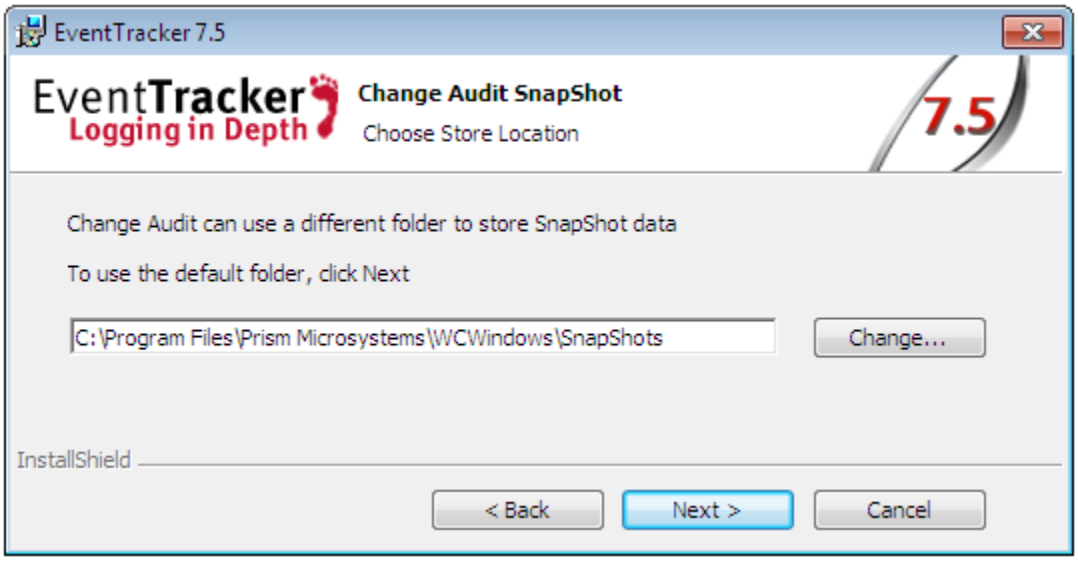


Figure 147

15. Click the **Next >** button to keep the default store location.
    (OR)
    Click the **Change** button to change the snapshot store location.

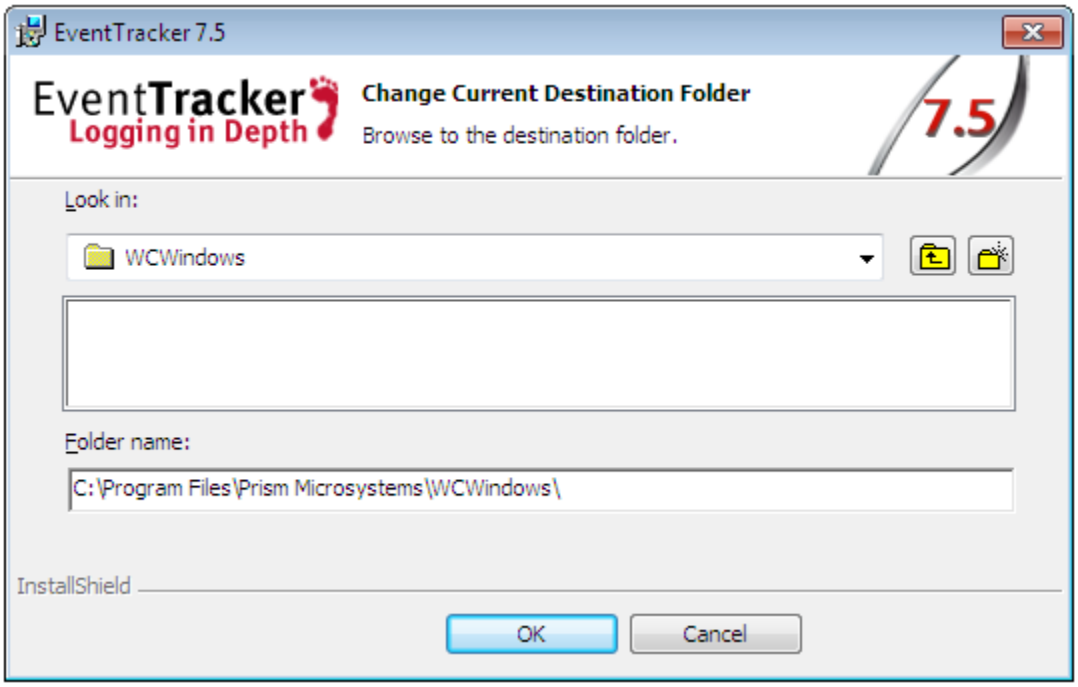


Figure 148

16. Browse the destination folder, and then click the **OK** button.

    NOTE:

    The Change Audit snapshot store location can be changed only during fresh install and if

snapshots are not retained during uninstall.

In case of upgrade, if the change audit snapshots are retained during product un-installation, then the snapshot store location path cannot be changed.

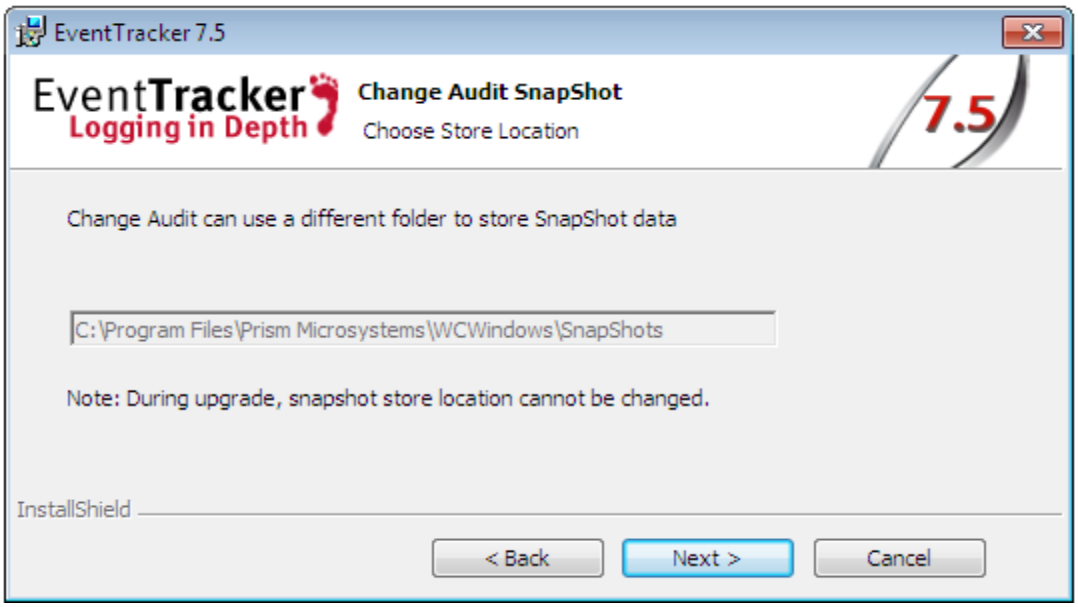


Figure 149

If you have not selected to install **Change Audit,** then InstallShield[R] Wizard displays the **Ready to Install the Program** screen.

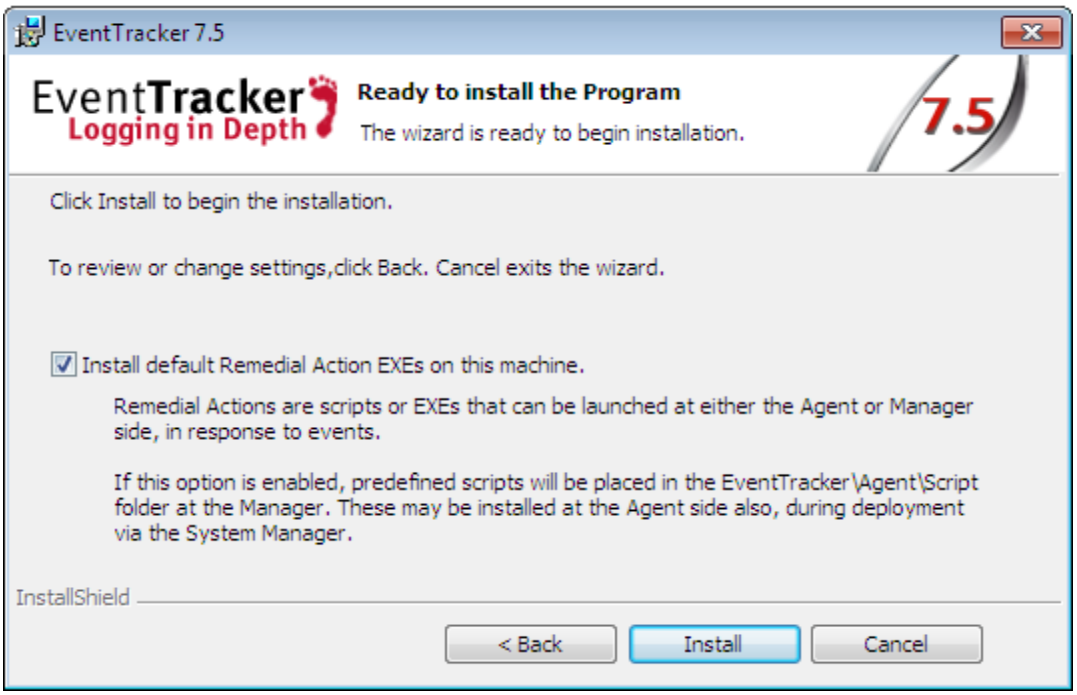

EventTracker 7.5
EventTracker
Logging in Depth
Ready to install the Program
The wizard is ready to begin installation.
7.5
Click Install to begin the installation.
To review or change settings,click Back. Cancel exits the wizard.
Install default Remedial Action EXEs on this machine.
Remedial Actions are scripts or EXEs that can be launched at either the Agent or Manager side, in response to events.
If this option is enabled, predefined scripts will be placed in the EventTracker\Agent\Script folder at the Manager. These may be installed at the Agent side also, during deployment via the System Manager.
InstallShield
< Back
Install
Cancel

Figure 150

17. Select the **Install Remedial Action EXEs on this machine** option.

    Remedial Action EXEs are copied to <InstallDir>\EventTracker\Agent\Script folder.

18. Select the **Install** button.

    InstallShield[R] Wizard installs the selected components.

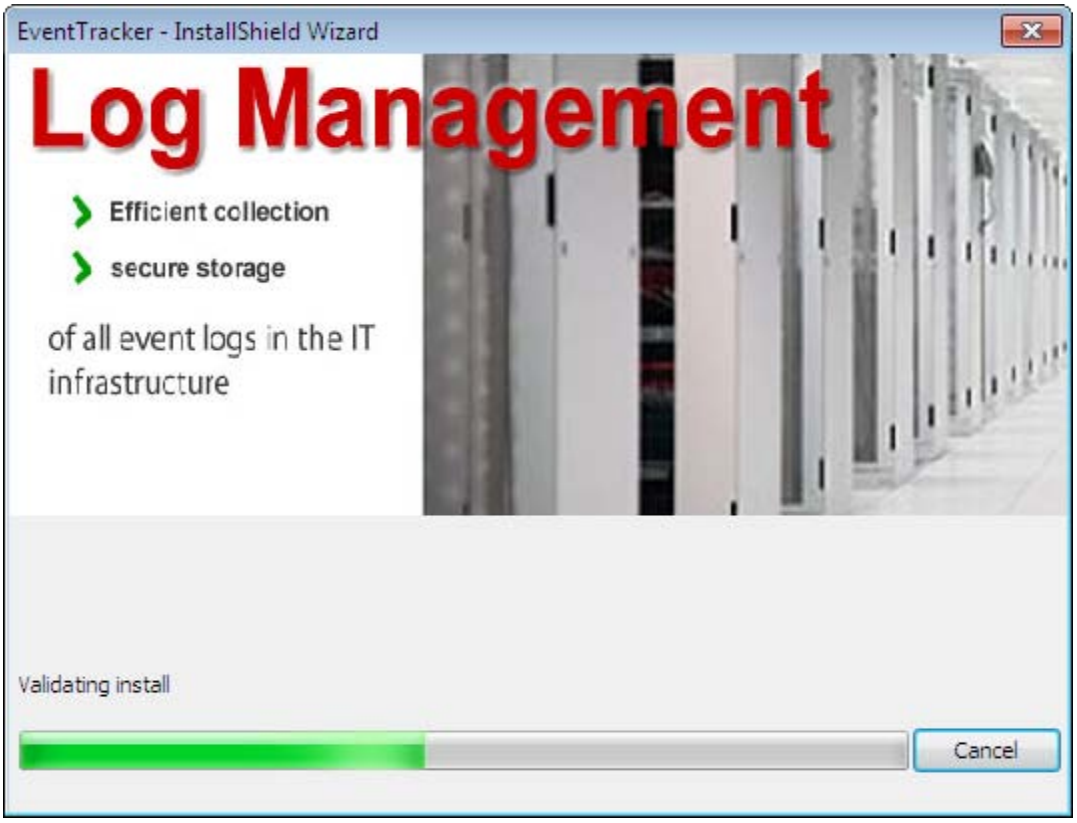


Figure 151

InstallShield[R] Wizard initializes the configuration settings required for proper operation of EventTracker. After initializing the necessary configuration settings, InstallShield[R] Wizard displays the **Basic configuration** dialog box.

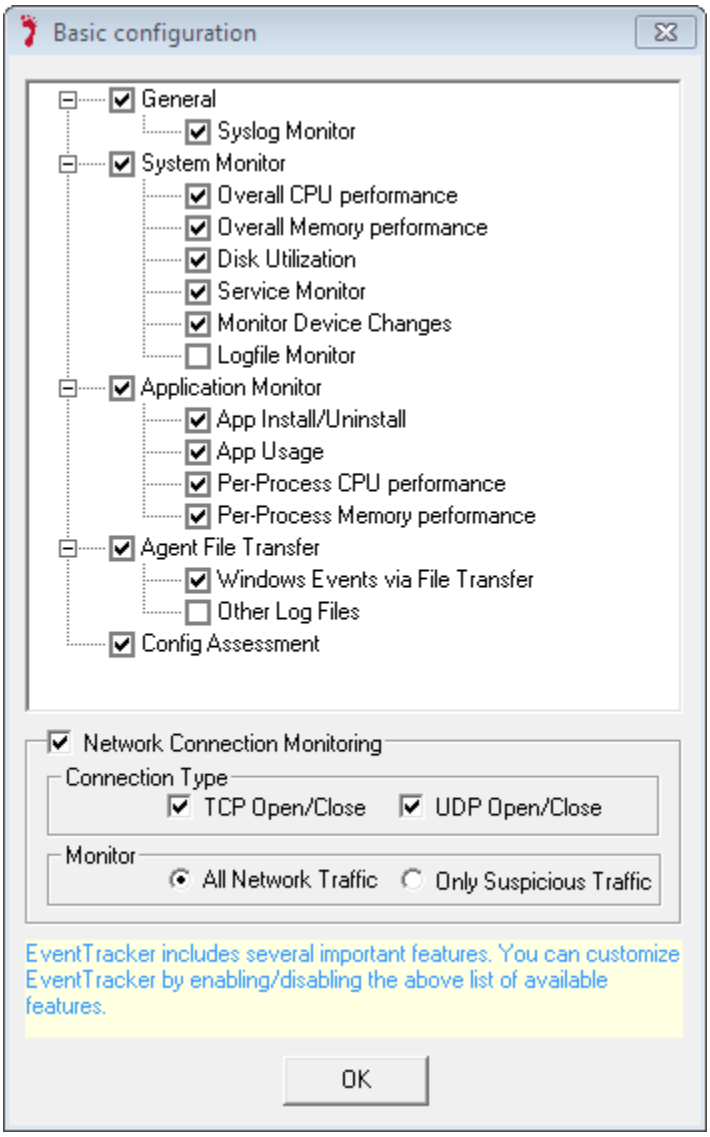


Figure 152

19. Select appropriate options, and then click **OK**.

    InstallShield Wizard displays the **Alert and Report generation settings** dialog box.

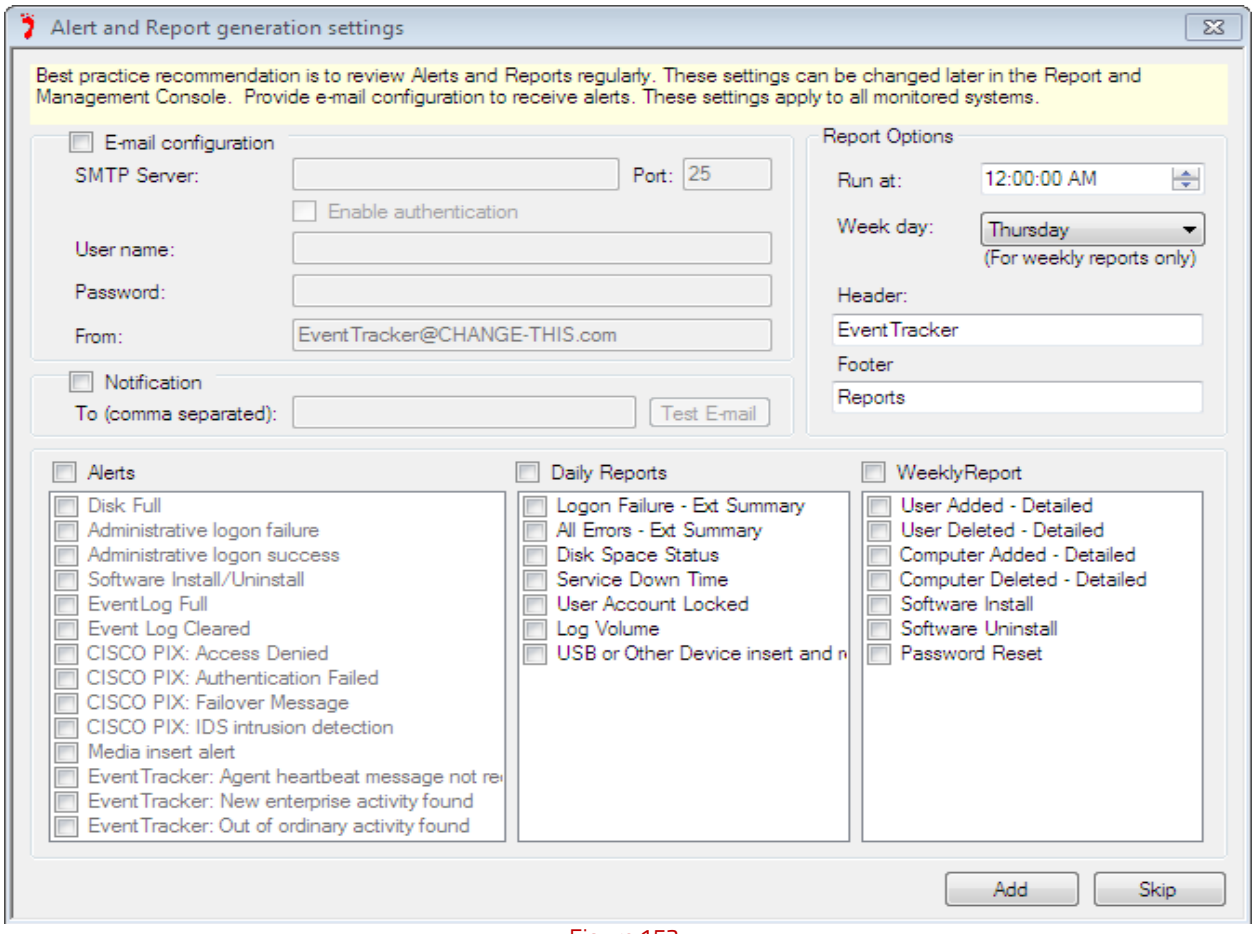


Figure 153

20. Select/enter appropriate data in the relevant fields, and then click **Add**.

    (OR)

    Click **Skip** if you do not wish to add the basic settings.

    InstallShield Wizard displays the last screen.

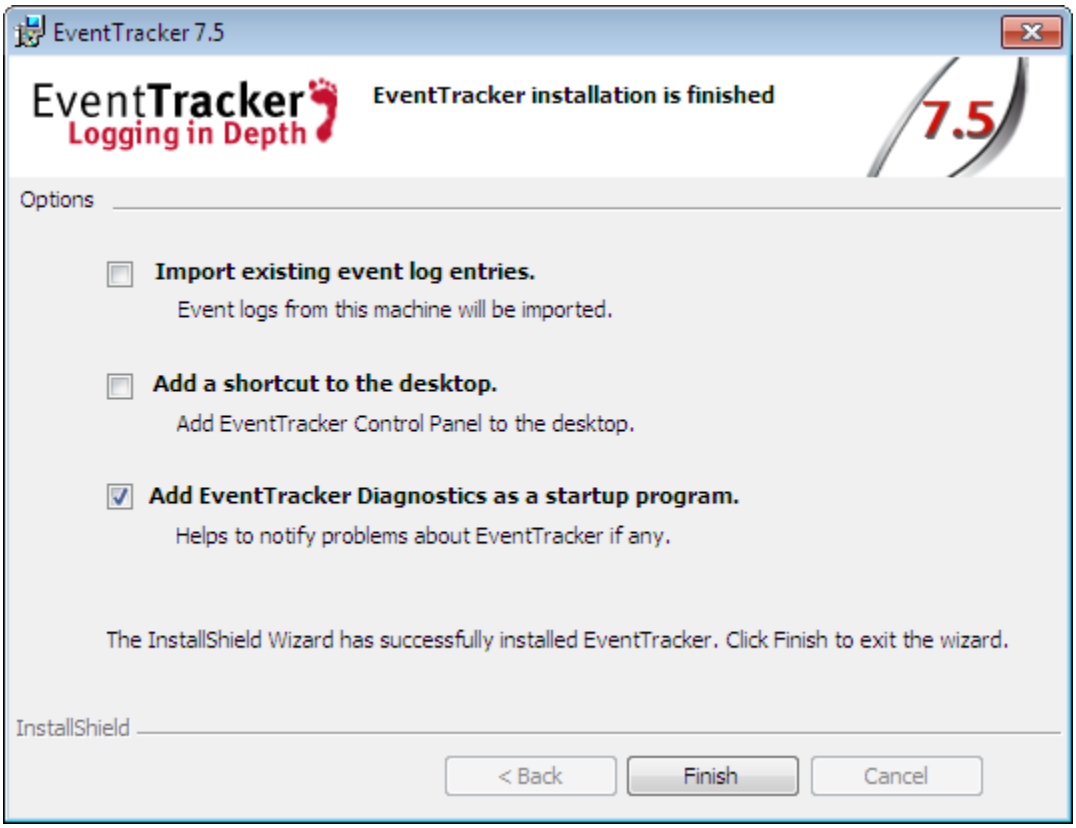

EventTracker 7.5
EventTracker
Logging in Depth
EventTracker installation is finished
7.5
Options
Import existing event log entries.
Event logs from this machine will be imported.
Add a shortcut to the desktop.
Add EventTracker Control Panel to the desktop.
Add EventTracker Diagnostics as a startup program.
Helps to notify problems about EventTracker if any.
The InstallShield Wizard has successfully installed EventTracker. Click Finish to exit the wizard.
InstallShield
< Back
Finish
Cancel

Figure 154

21. Click **Import existing event log entries** option to import event logs of EventTracker. Windows Security Alert message will be displayed if Firewall is on.

Windows Security Alert
To help protect your computer, Windows Firewall has blocked some features of this program.
Do you want to keep blocking this program?
Name: GetAllEvt PreVista Application
Publisher: Prism Microsystems, Inc
Keep Blocking
Unblock
Ask Me Later
Windows Firewall has blocked this program from accepting connections from the Internet or a network. If you recognize the program or trust the publisher, you can unblock it. When should I unblock a program?

Figure 155

Firewall blocks the incoming network connection, if getallevt.exe does not exist in the

Program and Services Exceptions and displays a notification.

22. Click **Unblock** for the getallevt.exe to import event logs.
23. Check **Add a shortcut to the desktop** option, to add the shortcuts to the EventTracker application on the desktop.

    Add EventTracker diagnostics as a startup program option is selected by default to notify problems about EventTracker, if any.
24. Click **Finish** to conclude the installation process.

    InstallShield[R] Wizard displays the **EventTracker Configuration** screen.

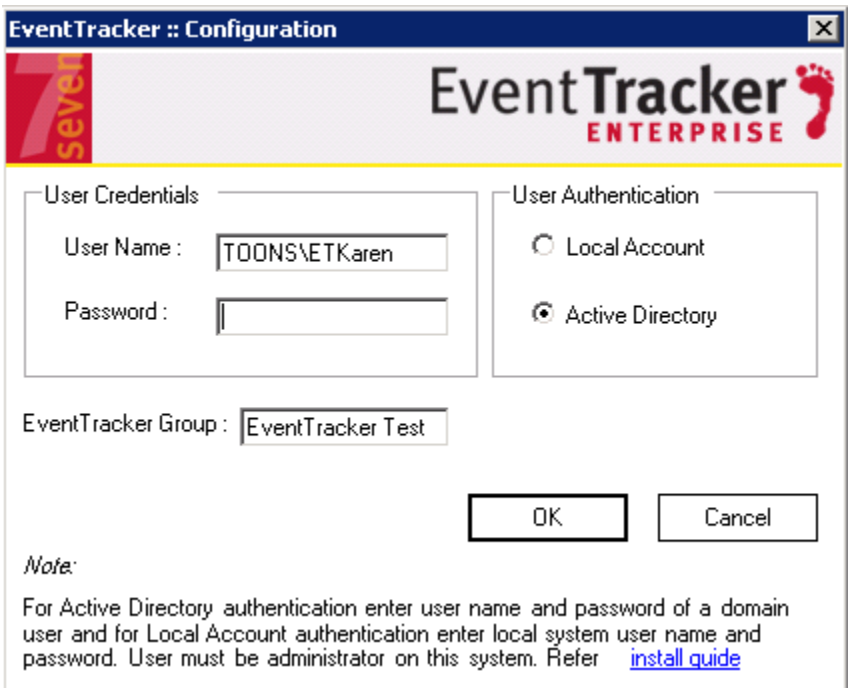


Figure 156

NOTE:

Make sure that you select/enter the correct **User Credentials, User Authentication** and **EventTracker Group** in order to login successfully.

25. Type valid user credentials in the **User Name** and **Password** fields respectively.

    NOTE:

    EventTracker services run under this account. By default, this user is assigned the 'Event Tracker Administrator' role and can login to EventTracker.
26. Select a **User Authentication** option.

    Local Account: Authentication is done locally on the computer where EventTracker is being installed. For more information see: Creating Local User and Group Accounts

Active Directory: Authentication is done in the Active Directory.

For more information, please refer "Create Active Directory User and Group Accounts".

27. Type the EventTracker group name in the **EventTracker Group** field.
28. Click **OK**.

    After successfully validating the user credentials, InstallShield[R] Wizard displays the **EventTracker Configuration** message box.

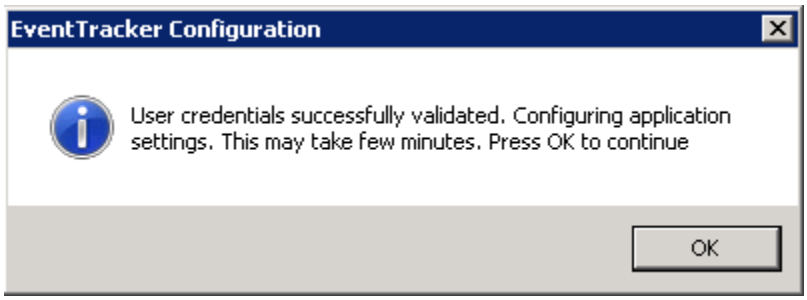

EventTracker Configuration
User credentials successfully validated. Configuring application settings. This may take few minutes. Press OK to continue
OK

Figure 157

29. Click **OK**.

    NOTE:

    If you change the system logon password, EventTracker logon password has to be updated. In order to synchronize the password, please update the same in **EventTracker Configuration.**

    a. To find '**EventTracker Configuration'**, select the **Start** button, select All **Programs**.

    b. Select **Prism Microsystems**, select **EventTracker**, and then select **EventTracker Configuration.**

    c. Enter appropriate credentials and then select the **OK** button**.**

User Permission on SQL Server

Users trying to install EventTracker should have sysadmin privilege on respective SQL Server 2005 / 2008 / 2008 R2 / 2012.

NOTE:

In SQL 2008 / 2008 R2 / 2012, please make sure that sysadmin privilege has been granted to NT AUTHORITY\SYSTEM.

Scenario 1:

If **NT AUTHORITY\SYSTEM** is not available under **Security -> Logins** then it has to be created. The steps are mentioned below.

A) Select the **Start** button, select **Microsoft SQL Server (2008 / 2008 R2 / 2012)** and then select **Microsoft SQL Server Management Studio**.

B) Expand **Security** node, right click **Logins** node and then select **New Login.**
Login – New window displays.

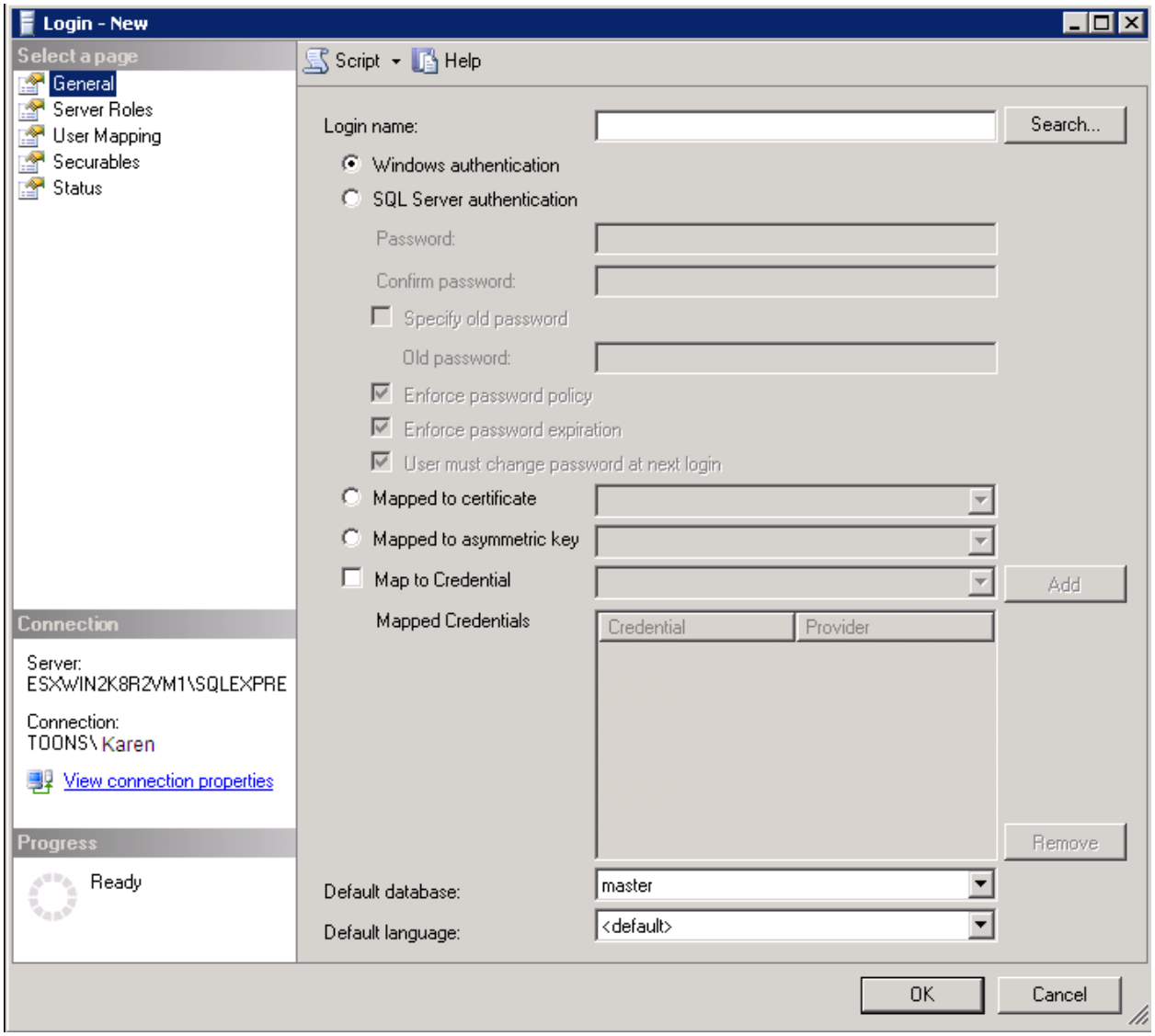


Figure 158

C) Select the **Search...** button.

Select User or Group window displays. The location should be your local system.

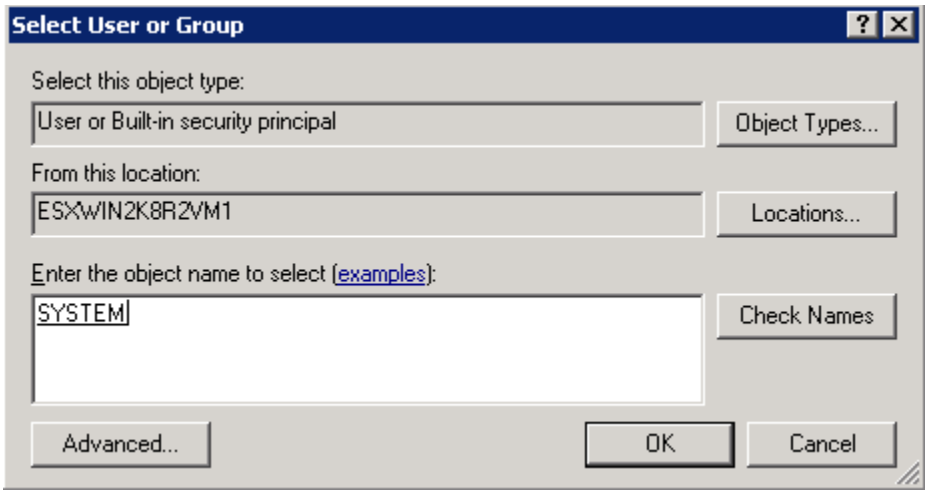


Figure 159

D) In **Enter the object name to select** box, type **system** and then select **Check Names**.

E) Select the **OK** button.

NT AUTHORITY\SYSTEM displays in Login window.

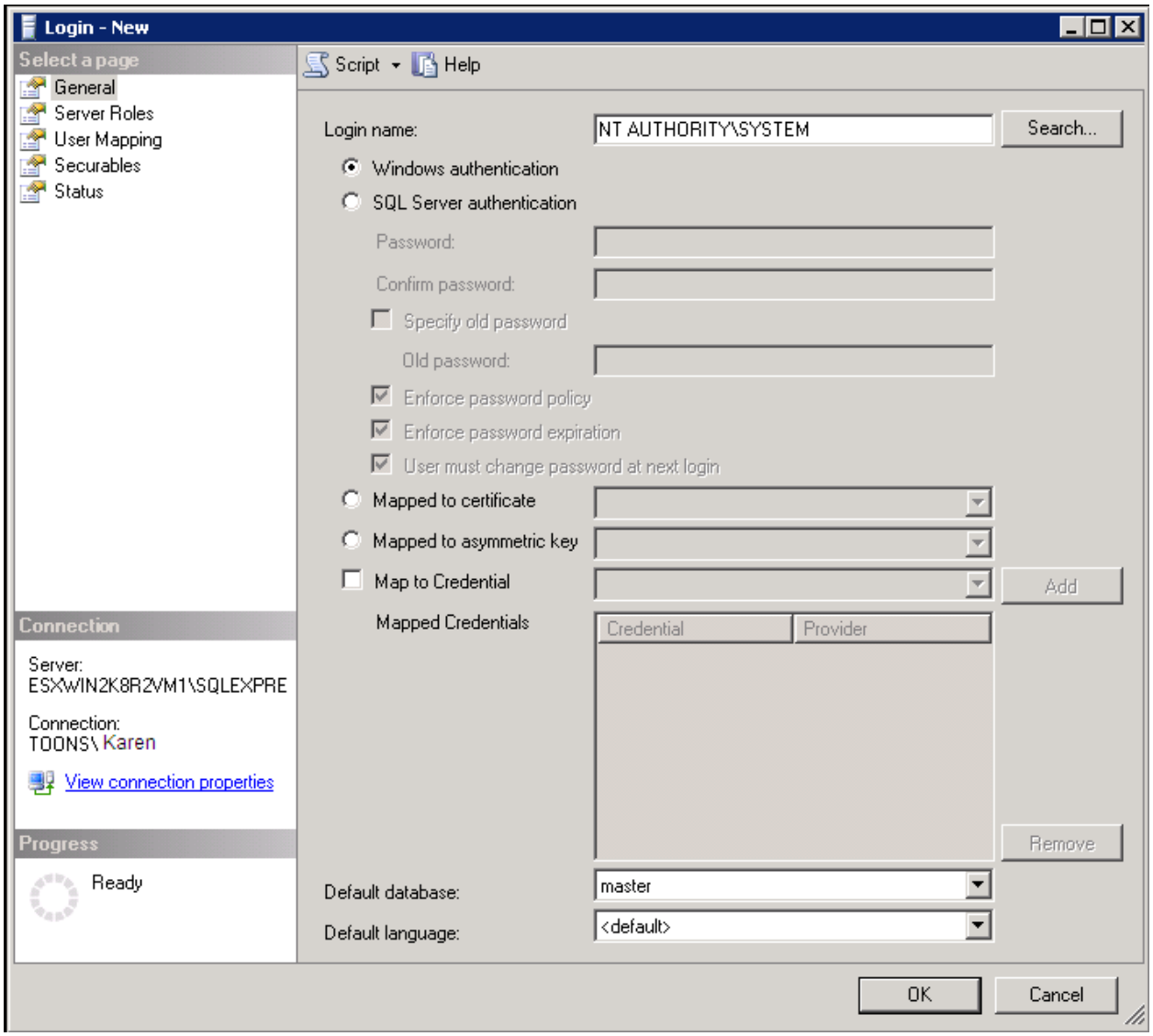


Figure 160

F) In **Select a page** pane, select **Server Roles** and then select **sysadmin** option.

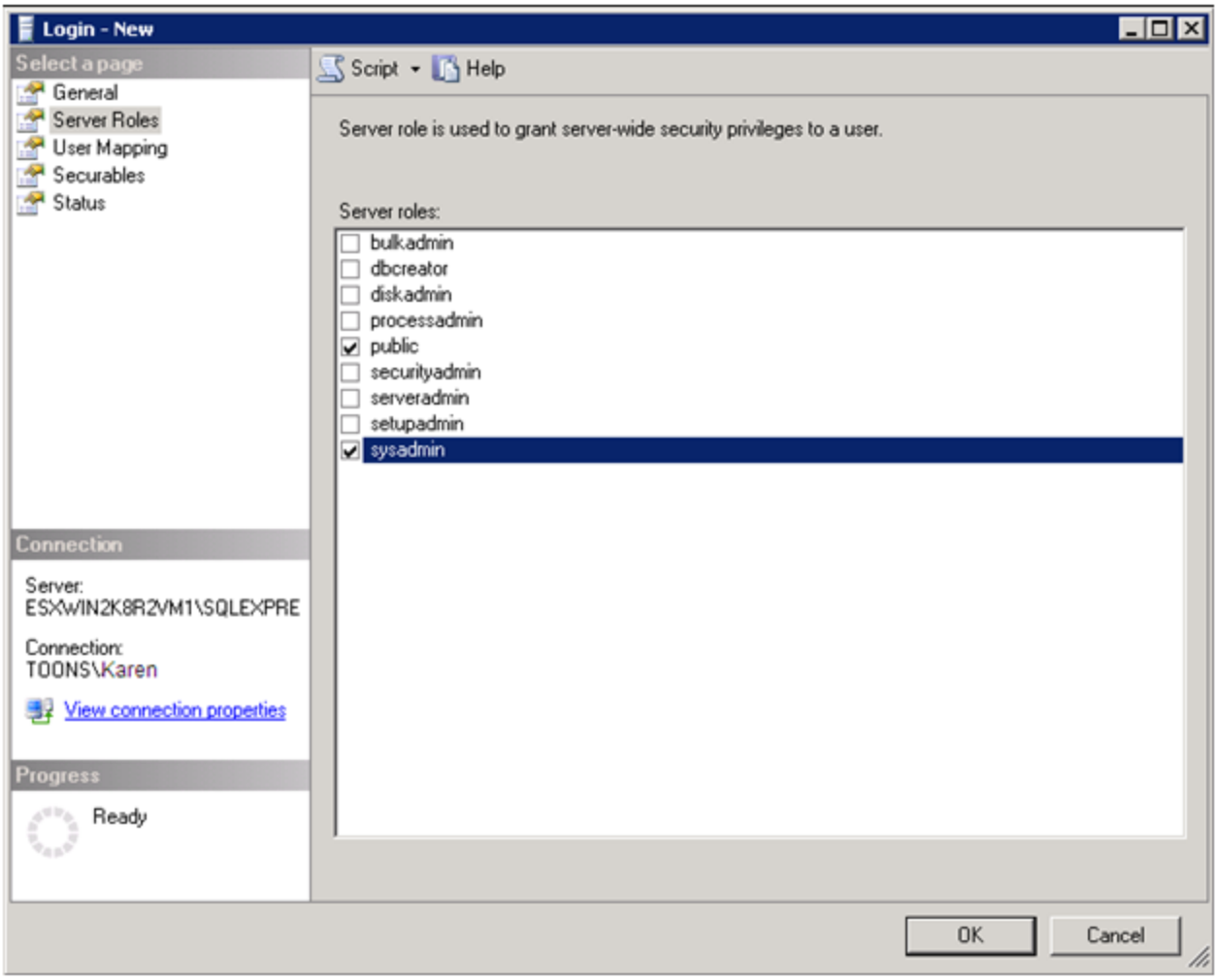


Figure 161

G) Select the **OK** button.

Scenario 2:

If **NT AUTHORITY\SYSTEM** is already available under **Security -> Logins** then please follow the steps mentioned below to grant sysadmin permission.

a) Expand **Security** node, expand **Logins** node.

b) Right click **NT AUTHORITY\SYSTEM** and then select **Properties**.

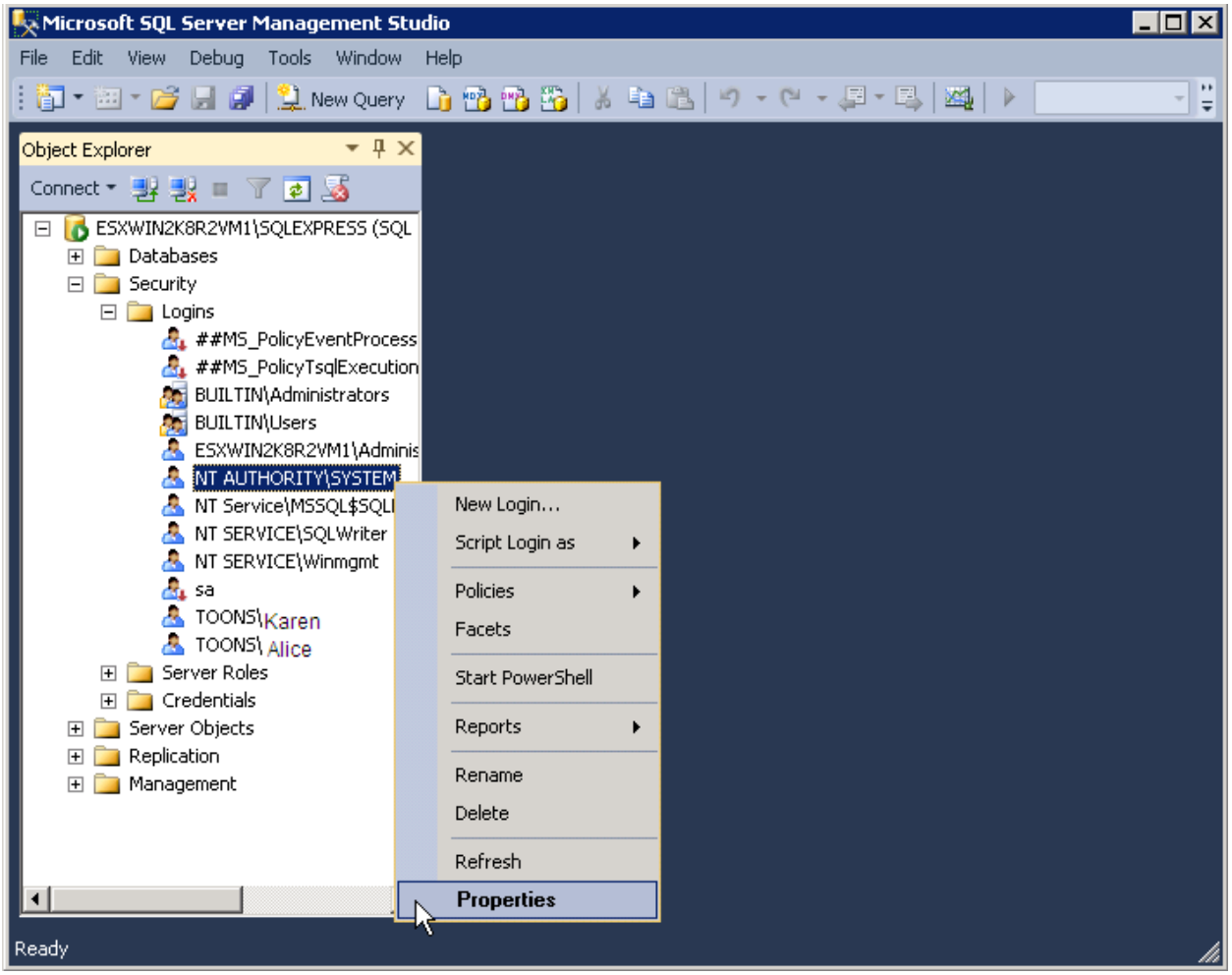


Figure 162

c) Select **Server Roles** and then select **sysadmin**, if not selected.

Refer Figure 161.

Scenario 3:

To grant sysadmin privilege to an individual user or an administrators group, please follow the steps given below.

A) Expand **Security** node, right click **Logins** node and then select **New Login.**

B) Click the **Search** button.

Select User or Group window displays.

C) Select the **Object Types...** button, select **Groups**, and then select the **OK** button.

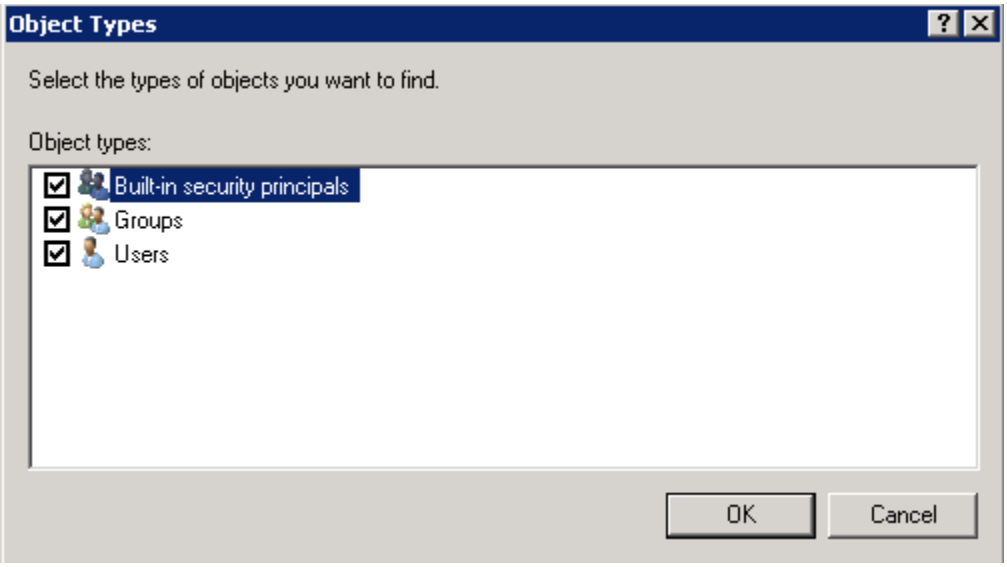


Figure 163

D) In **Enter the object name to select box**, enter 'administrators/username' and then click **Check Names**.

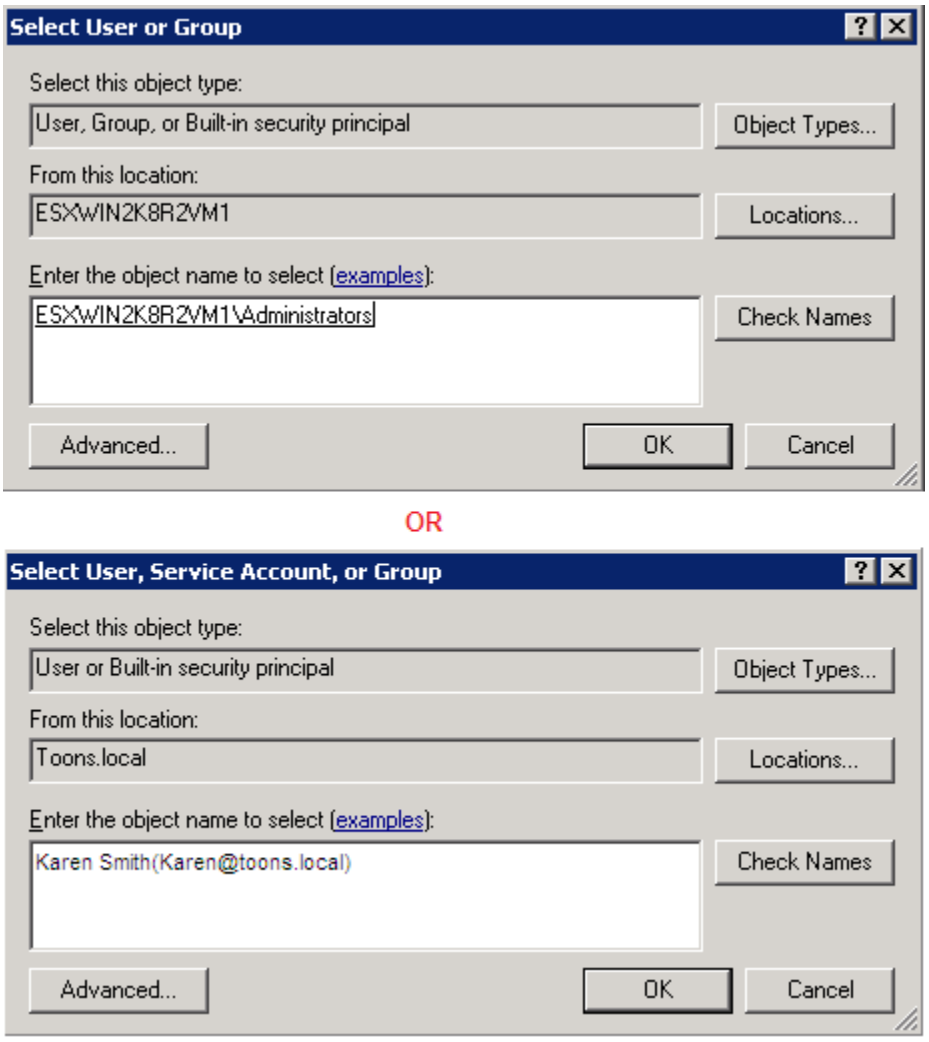


Figure 164

E) Click **OK**.

F) Select **Server Roles** and then select **sysadmin**.

Refer Figure 161.

G) Click **OK**.

NOTE:

If the SQL service is running on a different account apart from system and network account, then the user account on which SQL service is running should have full permission to the reports folder. In order to use persist flex data, EventVault Explorer search and Correl reports, **sysadmin** permissions is required since SQL data base is created for these reports.

1. To grant full permission on **Reports** folder, browse the path where EventTracker is installed i.e. \\<INSTALLDIR>\EventTracker.

2. Right click **Reports** folder, and then select **Properties.**

3. Select **Sharing** tab, and then select **Share this folder**.

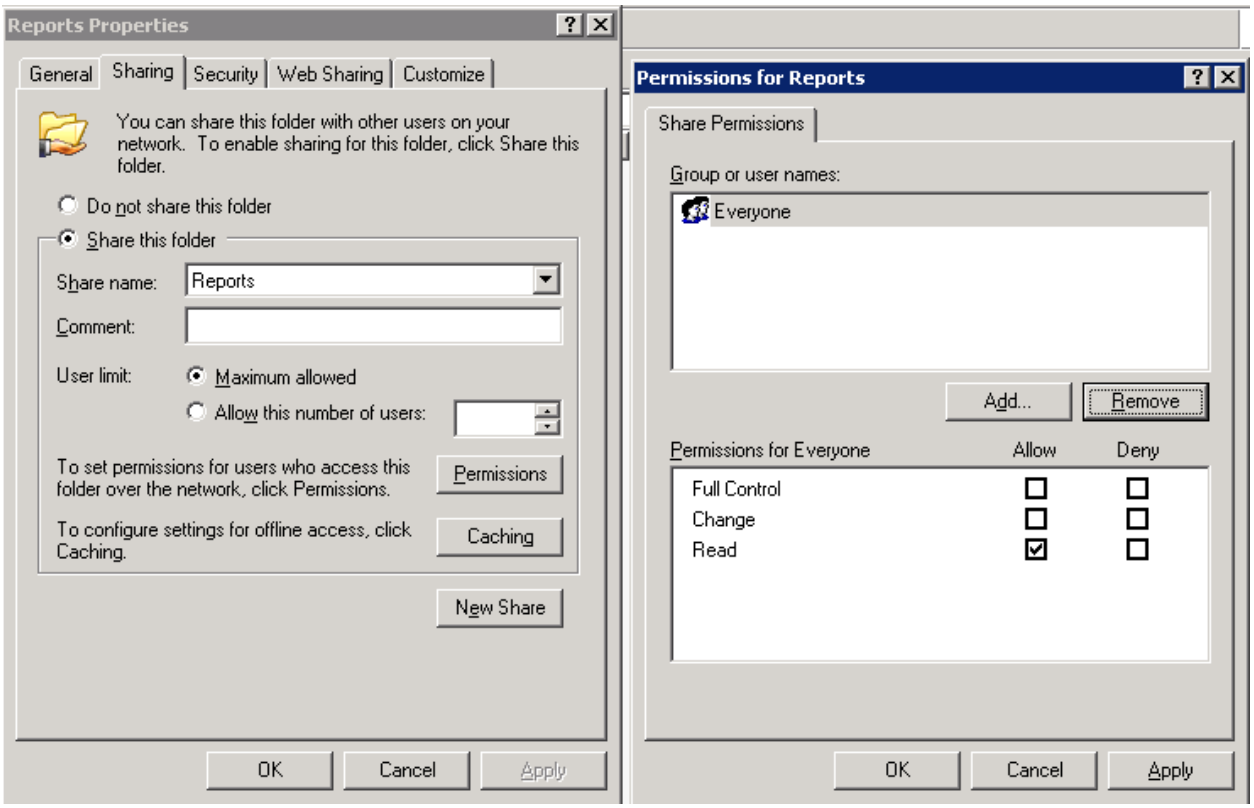


Figure 165

4. Select **Permissions**, and then select **Add...**.

   Select Users, Computers, or Groups displays.

5. In **Enter the object names to select** box, add the relevant users and then select **Check Names.**

6. Click **OK** and assign the relevant permissions.

7. Click **Apply** and then click **OK**.

8. Select **Security** tab, and then select **Add...**

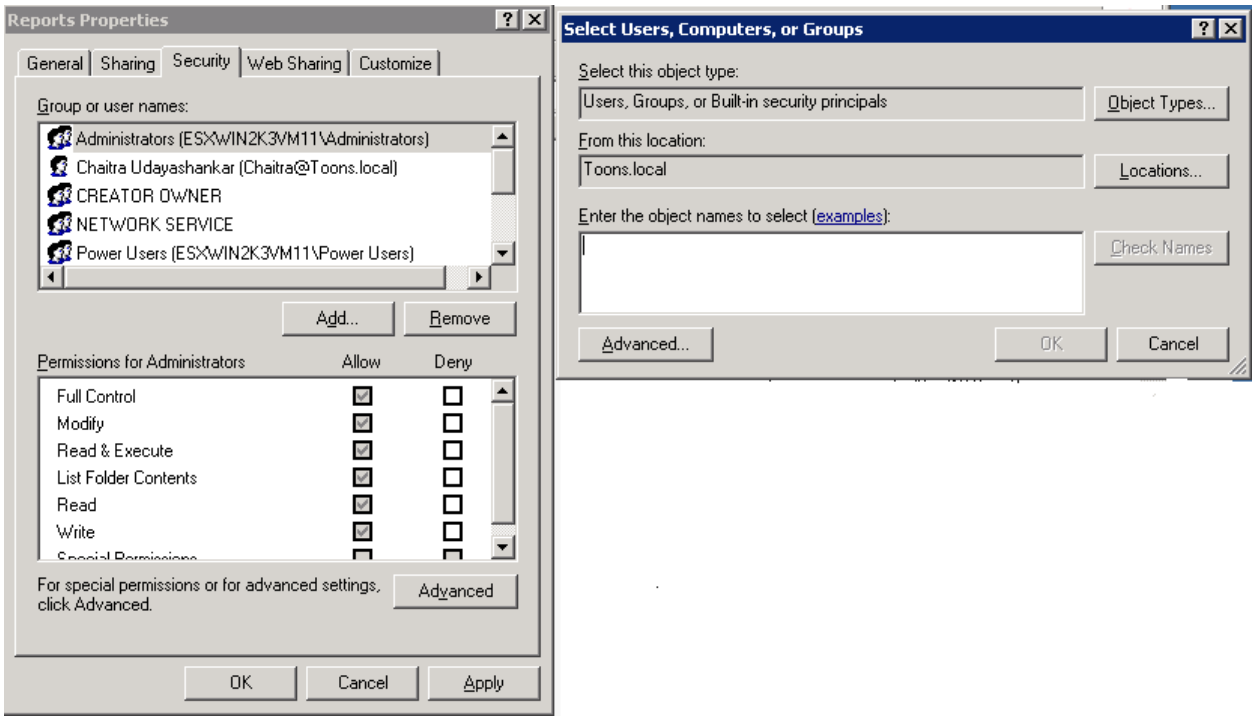


Figure 166

9. In **Enter the object names to select**, add the relevant users and then select **Check Names.** Assign full permission to appropriate users.

Deploy EventTracker Windows Agent

Pre-install Instructions for Windows Agent

- You MUST have Local Admin privileges on the remote systems where you want to remotely install the Agents.
- You can also install Agents with Local Admin privileges.
- Make sure that the systems that you are selecting to monitor are accessible through the network, have disks that are shared for the Admin, and have disk space up to 50MB that can be used by the Agent.
- If the remote system is accessed through a VPN with a slow line speed, the install may take time and it is recommended that you schedule your activities accordingly.
- To monitor a system that supports SYSLOG messages (e.g. Unix, Linux, and Cisco etc); configure that specific system to forward the SYSLOG messages to EventTracker Manager.

Pre-install Checklist for Windows Agent

The pre-installation checklist describes the specific settings, permissions, and privileges that are required for deploying EventTracker agent. Read the checklist before installation to ensure safe and smooth agent installation.

ENSURE	**User is a member of 'Local Administrators' group**
	MSI package installation is allowed
	User has 'Logon As Service' rights
	Network Discovery is enabled
	File sharing is allowed
	Access this computer from network
VERIFY	User has permission on 'Application install directory' (Folders and sub folders).
	User must have create service permission on the target system(SCM-service control manager)
	User has Read/Write permission on windows registry.
	User has permission to Admin share(C$) of Target systems and C$ should be accessible from EventTracker Manager system.

Table 6

Different methods to install EventTracker Agents

There are 2 methods to deploy EventTracker Agents

a. Using the System Manager that is installed as part of the EventTracker Manager. From this System Manager, EventTracker Agents can be deployed onto all computers identified as EventTracker Agents.

(OR)

b. Using the Manual Agent Installation package on all computers identified as EventTracker Agents.

Deploy EventTracker Windows Agent via System Manager

Installation procedure is identical for Windows XP/Vista/7/2003/2008/2008 R2/8/2012/2012 R2 (v7.5 Build 29 and above) systems.

1. Select the **Start** button, select **All Programs**, and then select **Prism Microsystems.**
2. Select **EventTracker,** and then select **EventTracker Enterprise**.

   EventTracker displays the login page.
3. Logon with valid user credentials.

   EventTracker displays the **Incident** dashboard.
4. Click the **Admin** drop-down list at the upper-right corner, and then select **Systems**.

   EventTracker displays the Systems manager page.

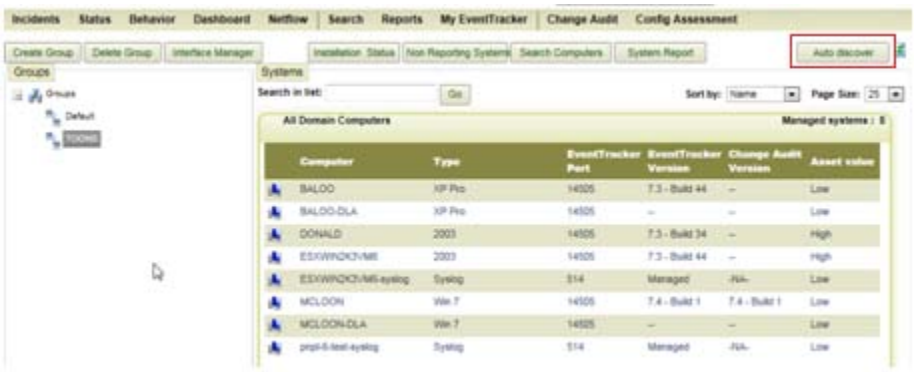


Figure 167

This console displays the list of systems that are members of all trusted domains provided if **Auto Discover** is ON. Otherwise only EventTracker Manager system will be displayed. It will also indicate the operating system type, asset value, port number, and managed system status through which the agent communicates with the 'EventTracker Receiver'.

5. Right-click the system group on the right-pane in which the target systems exist.

   EventTracker displays the shortcut menu.

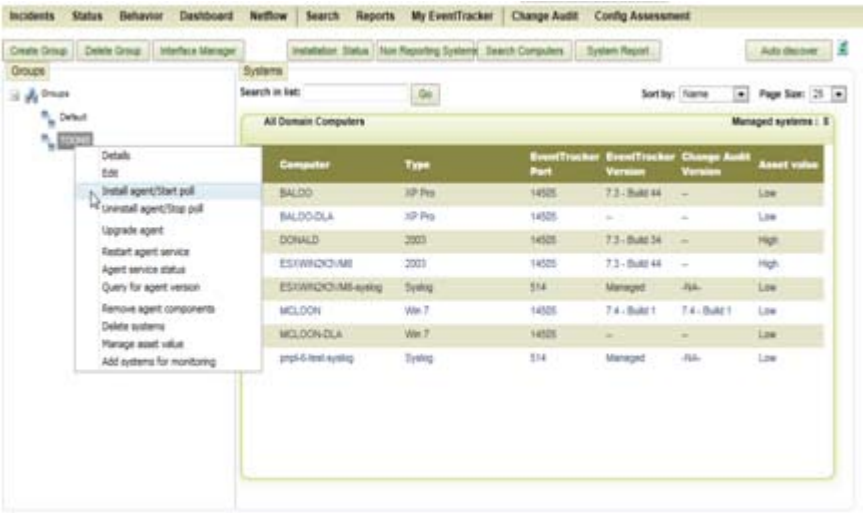


Figure 168

6. From the shortcut menu, click the **Install agent/Start poll** option.

   EventTracker displays the **Install agent/Start poll** dialog box.

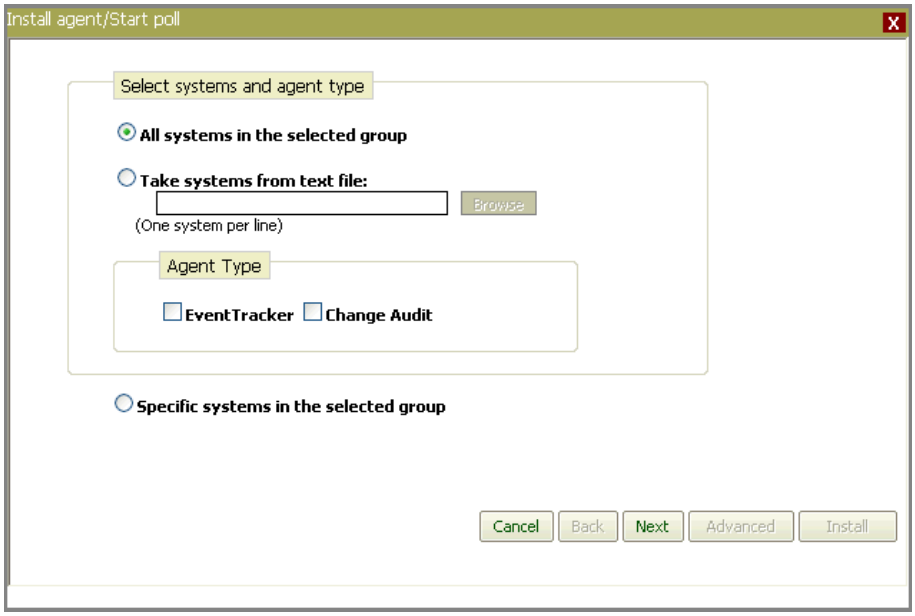


Figure 169

There are various options to **Select systems and agent type.** They are

- All Systems in selected group
- Take systems from text file
- Specific systems in the selected group

Details are given in the below table.

Option	To
All systems in the selected group	Click this option to install agents on all the systems present in the selected group.
Take systems from the text file	Create a text file containing agent system names on which the agent is to be installed. The text file should contain one system name per line. If you select this option then browse the text file to select the agent system names.
Agent type	Select the agent type to be Installed
Specific systems in the selected group	Out of all the systems present in the group, select specific system(s) to install the agent.

7. Click **Next.**

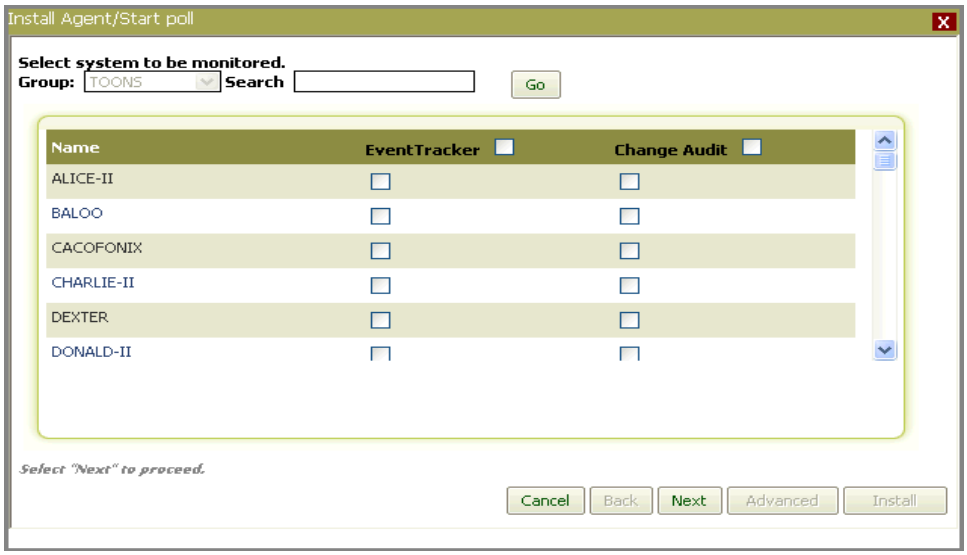


Figure 170

8. To install **EventTracker/Change Audit Agent** on all the system present in the domain, select the respective **EventTracker/Change Audit** option.

(OR)

Select the respective check box against the systems where you wish to deploy the EventTracker/Change Audit agent.

(OR)

In the **System** manager page, move the mouse pointer over the system where you wish to install the agent.

a) Click the dropdown.

EventTracker displays the drop-down list.

b) Click **Install agent/ Start poll**.

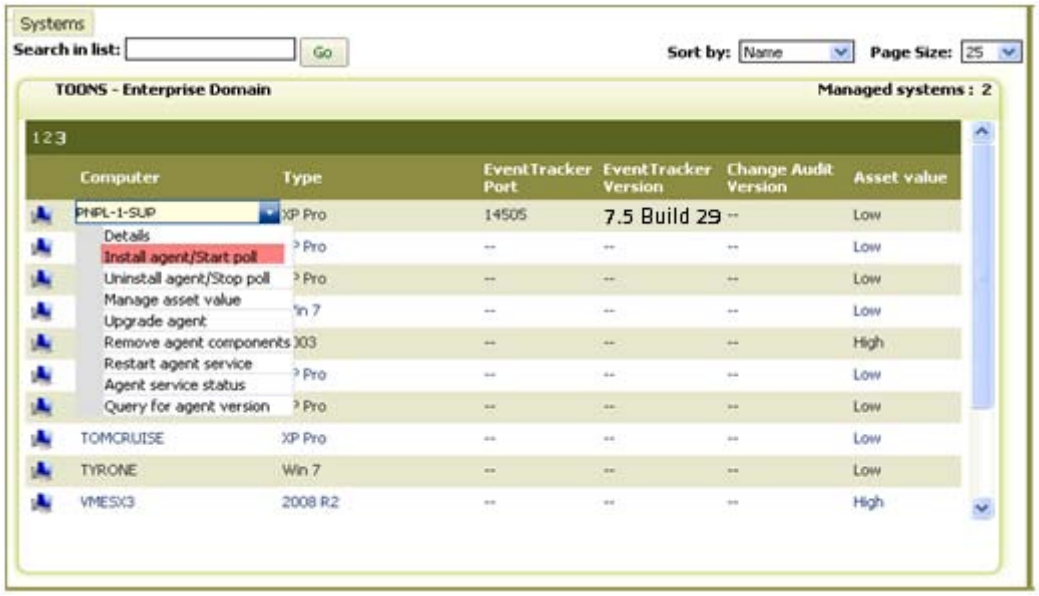


Figure 171

EventTracker displays the **Install Agent/Start poll** dialog box.

Figure 172

c) Check the **EventTracker** option to install EventTracker agent.

d) Check the **Change Audit** option to install Change Audit agent.

9. Click **Next**.

10. Select **EventTracker Agent Type i.e. Agent based (Full Featured) / Agent-less (limited feature)*** option.

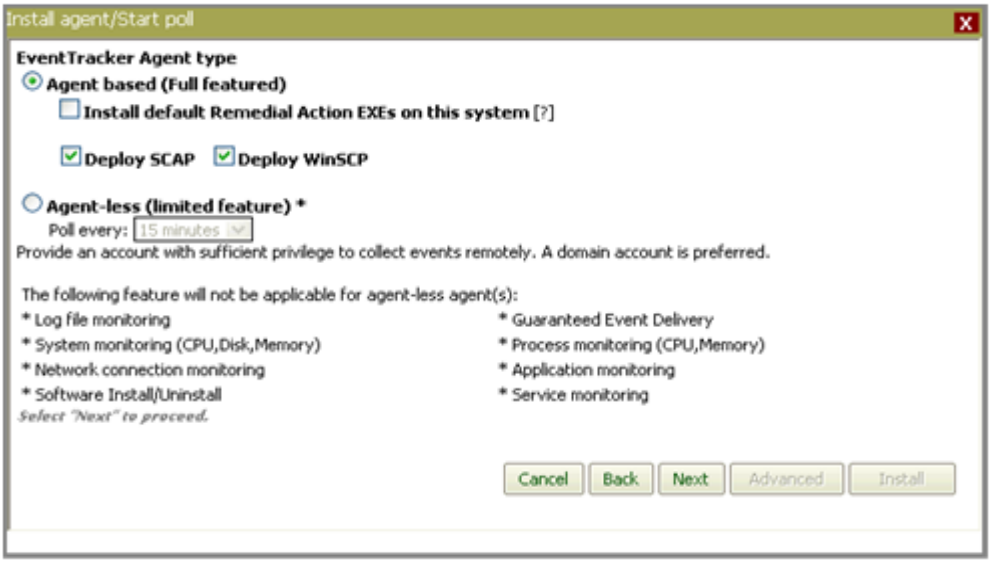


Figure 173

Agent based (Full featured)	
Install default Remedial Action EXEs on this system	**Remedial Actions** are scripts or executable files that can be launched at either the agent or the manager side, in response to events. If this option is enabled, predefined scripts will be placed in the EventTracker\Agent\Script folder at the manager side. These may be installed at the agent side also, during deployment via the **System** manager.
Deploy SCAP	Provides an option to install SCAP components to remote machines while deploying agent(s).
Deploy WinSCP	Provides an option to install WinSCP components to remote machines while deploying agent(s).
Agentless (limited feature)	
Poll Every	By default, the frequency is set to 15 min to receive events from the remote agent system. You can change the poll frequency as per the requirement.

11. If agent type is selected as '**Agent based (Full Featured)**', then remedial actions EXEs can be installed on the system.

    i. Select the **Install default Remedial Action EXEs on this system** check box to install remedial action scripts.

    EventTracker displays a message box.

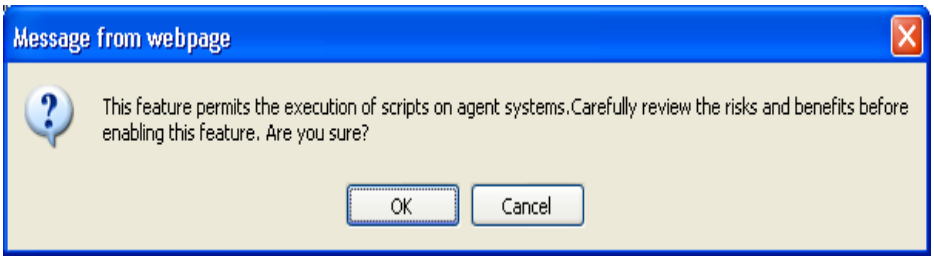

Message from webpage
This feature permits the execution of scripts on agent systems.Carefully review the risks and benefits before enabling this feature. Are you sure?
OK
Cancel

Figure 174

NOTE:

'Install default Remedial Action EXEs on this system' option is available for 'Agent based (Full featured)' installation.

    ii. Click **OK** to install remedial action EXEs

(OR)

Click **Cancel** to not to install remedial action EXEs.

iii. Click **Next**.

EventTracker displays the Install agent/Start poll dialog box with default client installation path on the remote computer.

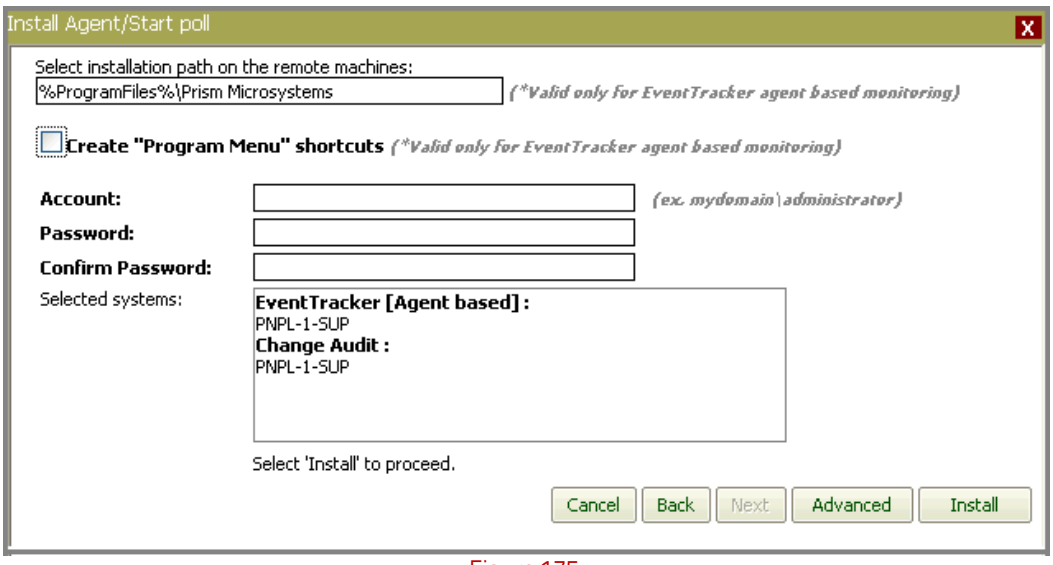


Figure 175

12. To install the agent in a different drive apart from the default one, type the new installation path in the **Select installation path on the remote machines** field.

13. Check the **Create "Program Menu" shortcuts** option to create shortcuts.

14. Enter valid **Account** name and **Password**.

15. Reenter the password in **Confirm Password**.

16. Click **Install**.

    The agent will be installed on the selected machine with the default etaconfig.ini configuration.

    (OR)

    a) To set a more specific configuration, click **Advanced**.

       The **Default** option is selected by default to apply manager side 'Agent configuration' settings (etaconfig.ini).

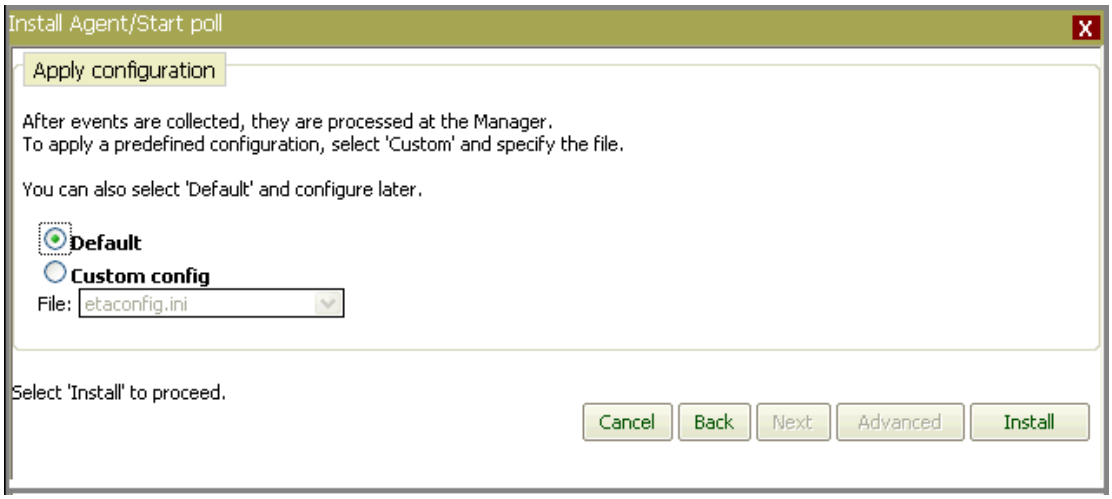


Figure 176

b) Select **Default** or **Custom config** option to select a custom configuration file as per the requirement.

The custom configuration will provide you the templates which you have created in Agent configuration and two more predefined templates.

You can select the template of your choice.
etaconfig_Servers.ini: This predefined template contains the ideal server configurations which can be applied to the selected agent system.

etaconfig_Workstations.ini: This predefined template contains the ideal workstation configurations which can be applied to the selected agent system. This option disables the 'Offline event sending' option.

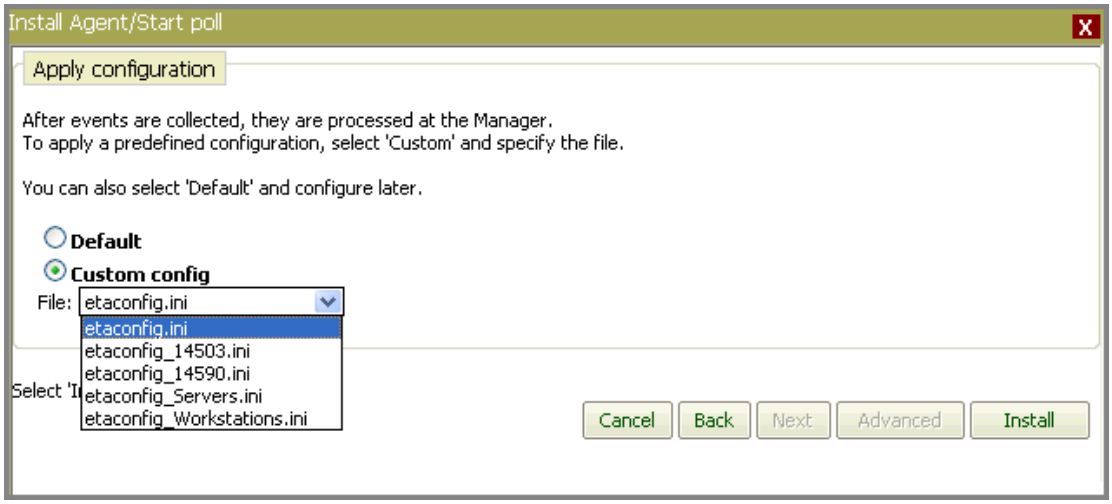


Figure 177

NOTE:

In case you select etaconfig_Servers.ini, etaconfig_Workstations.ini, Manager Name will be

empty after installation. If you want to use any of the pre-defined configuration (i.e. etaconfig_Servers.ini, etaconfig_Workstations.ini) you have to configure the Manager.

To configure Manager Name follow the steps given below.

i. Select **Admin** drop-down in EventTracker home page.

ii. Select **Windows Agent Config** and then select **Load Template**.

iii. Select the required file name i.e. etaconfig_Servers/etaconfig_Workstations accordingly. Select **Load**.

iv. In **EventTracker Managers** tab, select **Add**.

v. In **Add Destination** window, enter the relevant **Destination** and **Port**.

vi. In **Connect to Manager using** box**,** select **High Performance Mode (UDP)** or **Guaranteed Delivery Mode (TCP)** and then select the **OK** button.

c) Select the configuration file from the **File** dropdown, and then click the **Install** button. EventTracker displays the pop-up window with appropriate message.

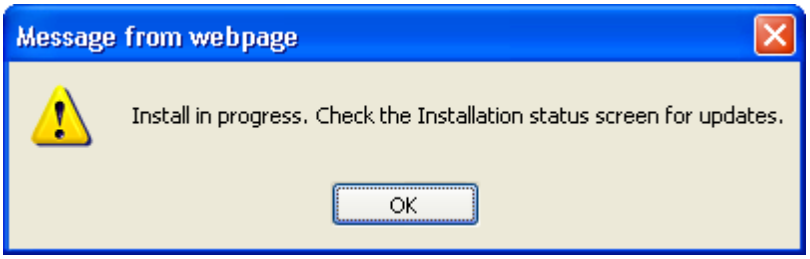


Figure 178

17. Click **OK.**

EventTracker displays **Installation Status** screen.

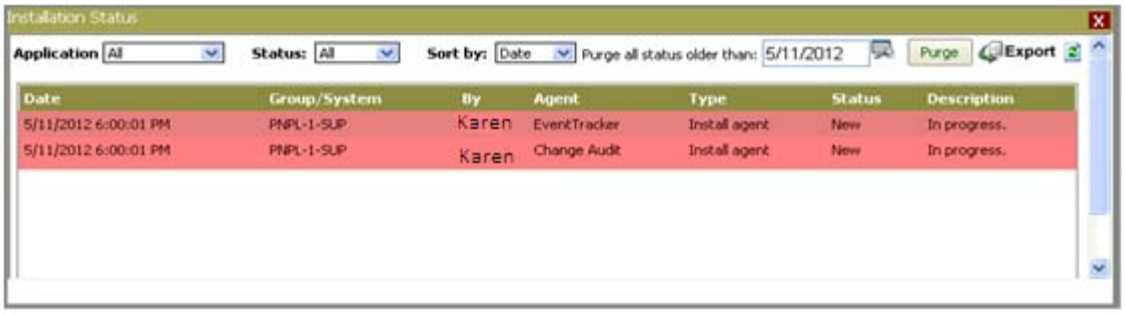


Figure 179

Select	To
Application	Sort the **Installation Status** results by the application installed. Available options are EventTracker & Change Audit.
Status	Sort the **Installation Status** results by status of the application installed. Available options are All, New, Success, and Failed.
Sort by	Sort the **Installation Status** results by **Date** application was installed /on which **System** it is installed / **Type** of activity performed/ **Status** of the application.
Purge all status older than	Remove the older installation status details from the list.
Export	Export the 'System Status' into **Excel** format

18. Click **Refresh** to view the current status.

    (OR)

    Reopen the **Installation Status** dialog box to see the updated status.

19. Click **Close.**

20. Refresh the **System** manager.

Configure EventTracker Windows Agent

All configurations for agent(s) are set by default during installation. If you are interested in changing the default configuration settings, then

1. Click the **Admin** drop-down list at the upper-right corner.
2. Click the **Windows Agent Config**.

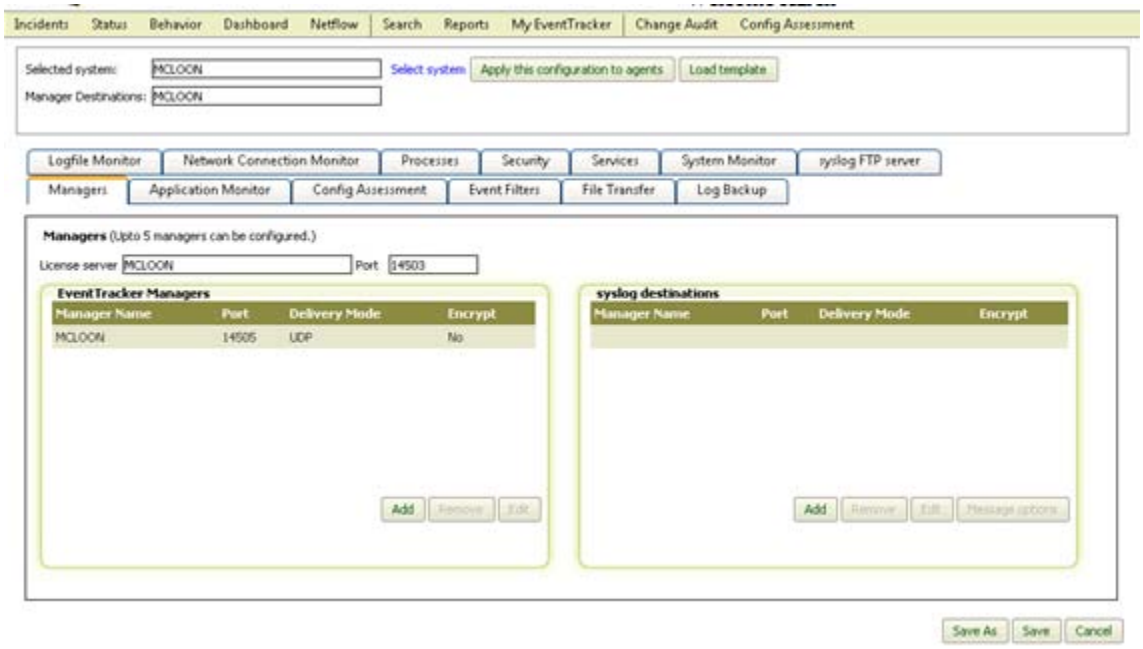


Figure 180

(OR)

1. Open **EventTracker Control Panel**.

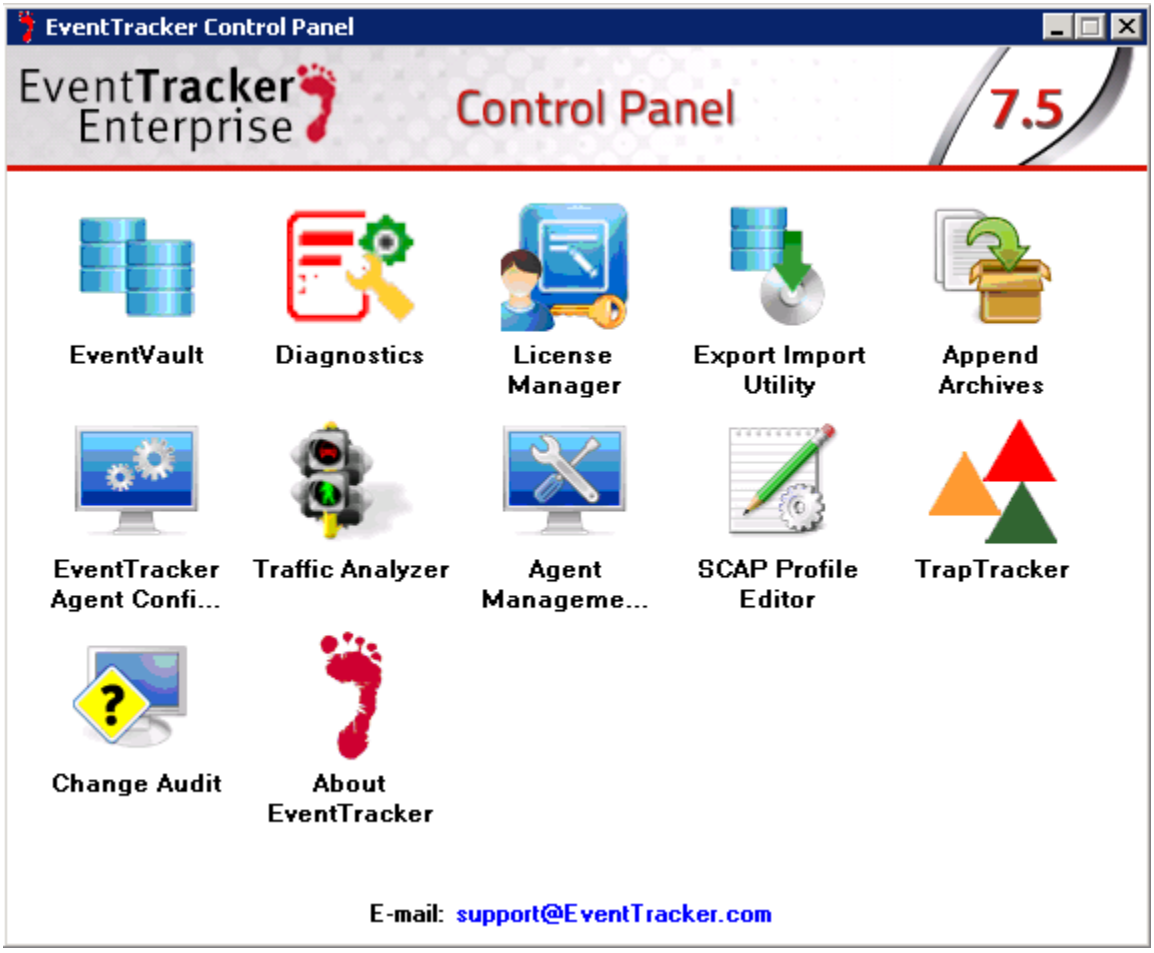


Figure 181

2. Double-click **EventTracker Agent Configuration**.

   EventTracker Agent Configuration window displays.

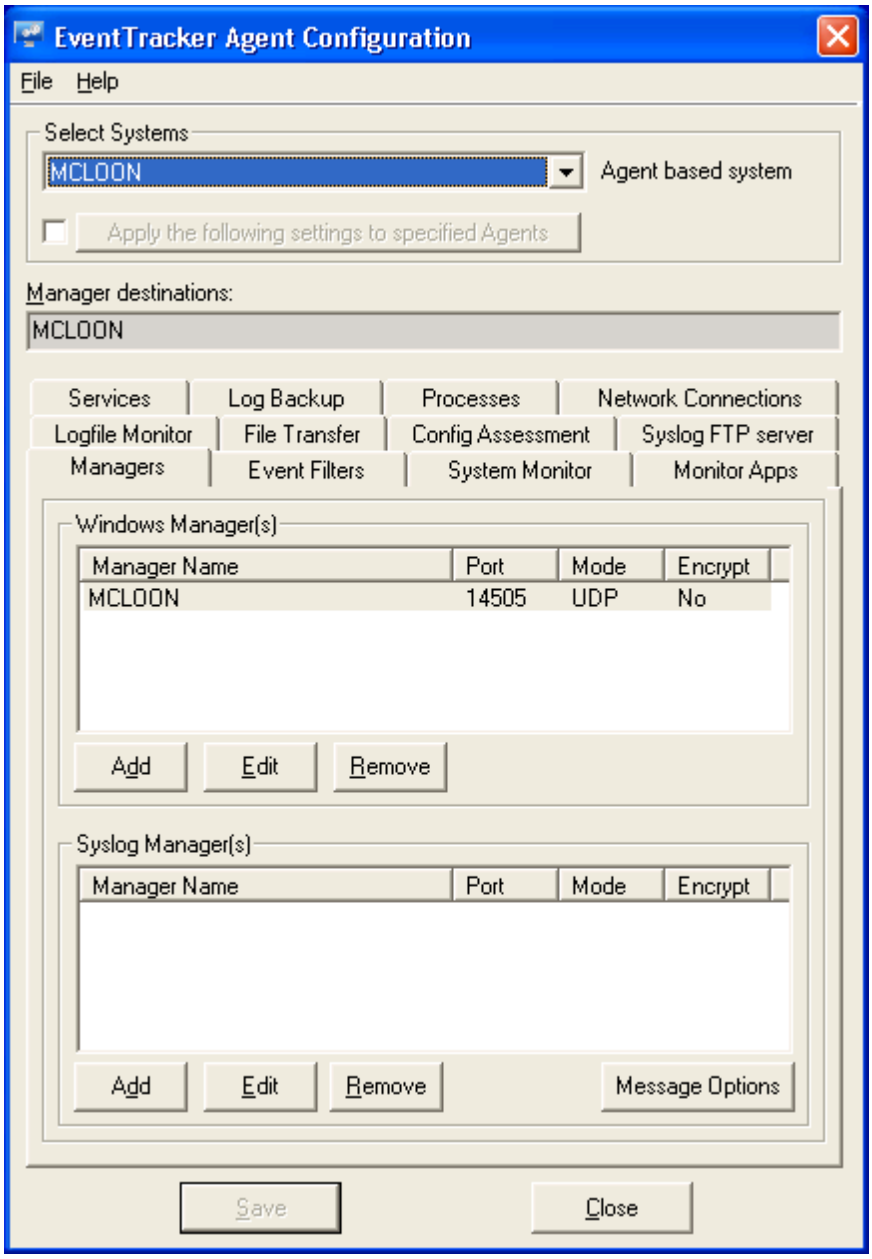


Figure 182

3. Click appropriate tabs and configure the agent as you wish.

Deploy EventTracker Windows Agent – Vista and Above

Prerequisites for Windows Agent – Vista and Above

Following are the mandatory settings you ought to do on Vista and above system(s) before you deploy an Agent.

1. By default, the Startup Type of Remote Registry is manual. Modify the Startup Type as Automatic and Start the service.
2. Enable File and Printer Sharing.
3. Turn on and enable Network Discovery.
4. To configure agent remotely, add port no 14506 TCP to Firewall Exceptions.
5. The user must be domain administrator, member of domain admin, or must be added to the local administrator group where the agent has to be deployed.

Install / Uninstall Vista and above Agent

Install and uninstall procedure for Vista and above Agent is identical to the procedures for other Windows Agents. No other additional configuration settings are required.

Agent Deployment

To install EventTracker Agent and Change Audit Agent please refer EventTracker Agent Deployment – User Manual.

Secure EventTracker

To secure EventTracker, please refer EventTracker Hardening Guide and OWASP Complaint EventTracker Guide.

Uninstall EventTracker Windows Agent

There are several methods to uninstall EventTracker Windows Agent. Few methods are mentioned below.

Uninstall EventTracker Windows Agent via Control Panel

1. Select the **Start** button, select **All Programs**, and then select **Control Panel**.

2. Select **Add or Remove Programs**, select **EventTrackerAgent**, and then select **Remove**.

   Windows Installer displays.

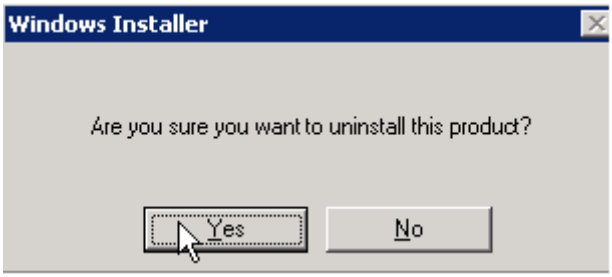


Figure 183

3. Select the **Yes** button.

   EventTracker window displays.

4. Select **Yes**/**No** as per the requirement.

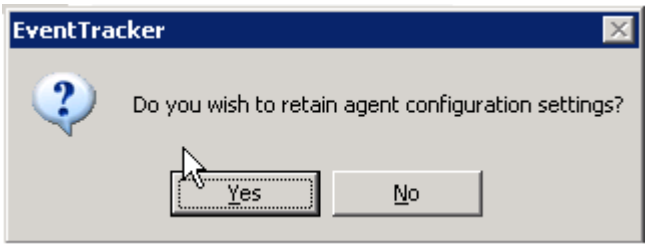


Figure 184

NOTE:

If you wish to retain the agent configuration settings, select the **Yes** button. If you do not wish to retain agent configuration settings, select the **No** button.

Uninstall EventTracker Windows Agent via System Manager

1) Click **Admin** drop down, select **Systems**.

2) Select the **Groups** or **Computer** name on which un-installation is required.

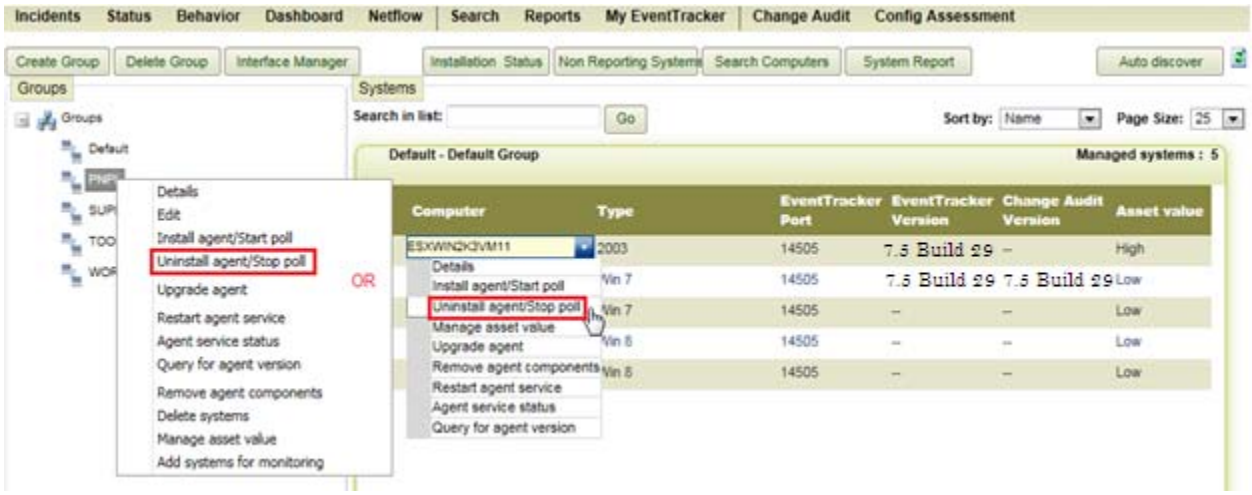


Figure 185

3) Select **Uninstall agent/Stop poll.**

Uninstall Remote agent(s)/Stop poll displays.

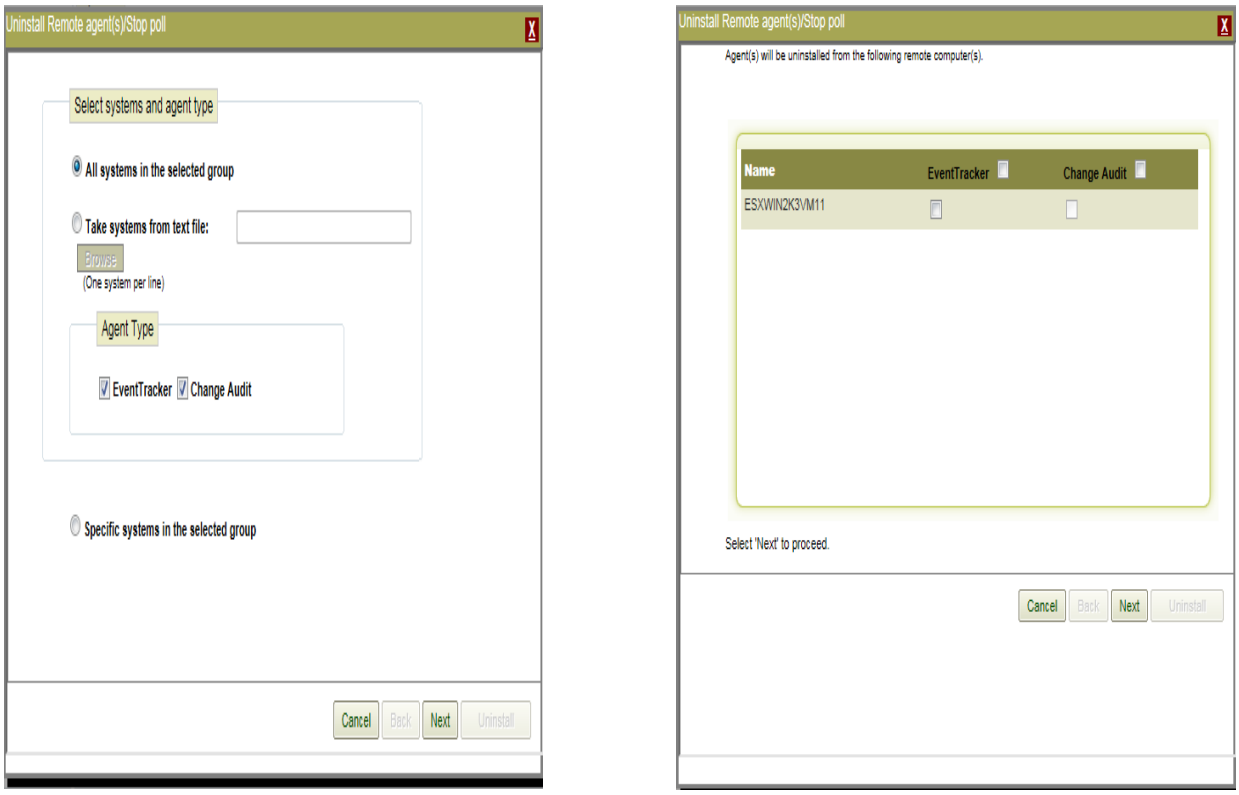


Figure 186

4) Select the required **EventTracker**, **Change Audit** options and then select the **Next** button.

Uninstall Remote agent(s)/Stop poll window displays.

Figure 187

5) Enter valid credentials and then select **Uninstall**.

Uninstall EventTracker

1. Select the **Start** button, select **All Programs**, and then select **Prism Microsystems**.
2. Select **EventTracker**, and then select **Uninstall EventTracker**.

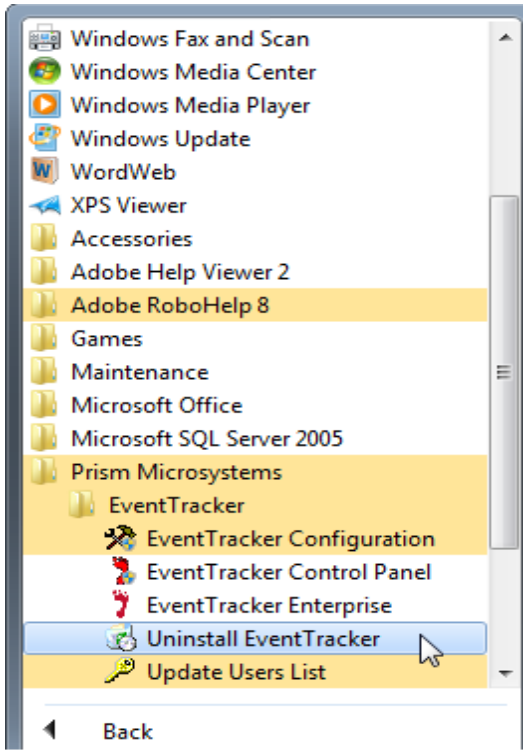


Figure 188

Windows Installer window appears displays.

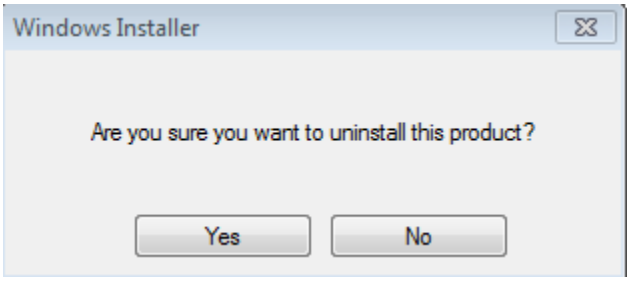


Figure 189

3. Select the **Yes** button.

EventTracker window displays.

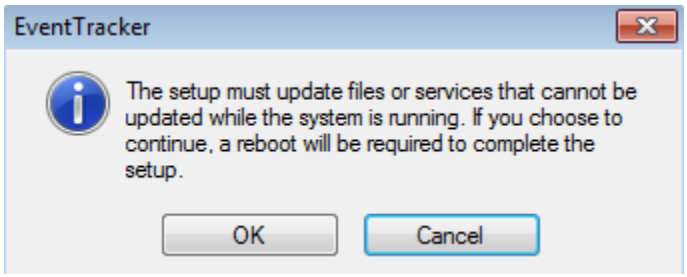

EventTracker
The setup must update files or services that cannot be updated while the system is running. If you choose to continue, a reboot will be required to complete the setup.
OK
Cancel

Figure 190

4. Select the **Ok** button.

   Uninstall EventTracker Enterprise window displays.

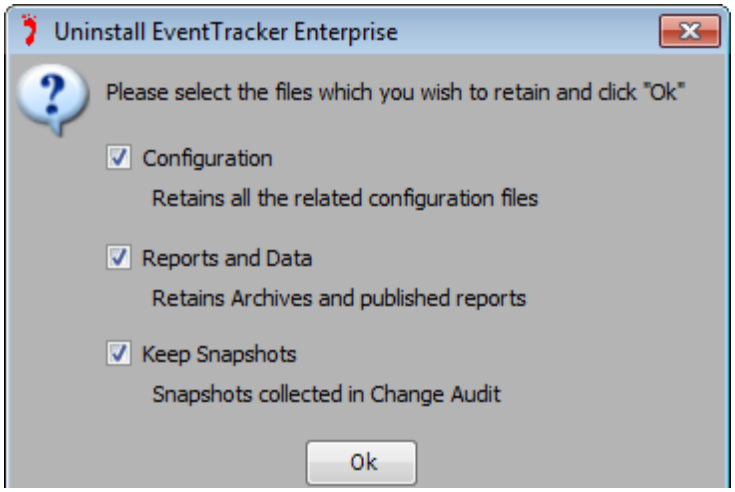

Uninstall EventTracker Enterprise
Please select the files which you wish to retain and click "Ok"
Configuration
Retains all the related configuration files
Reports and Data
Retains Archives and published reports
Keep Snapshots
Snapshots collected in Change Audit
Ok

Figure 191

NOTE:

In case you wish to retain **Configuration, Reports and Data, Snapshots** files then select the respective check box otherwise uncheck the options.

5. Select the **Ok** button.